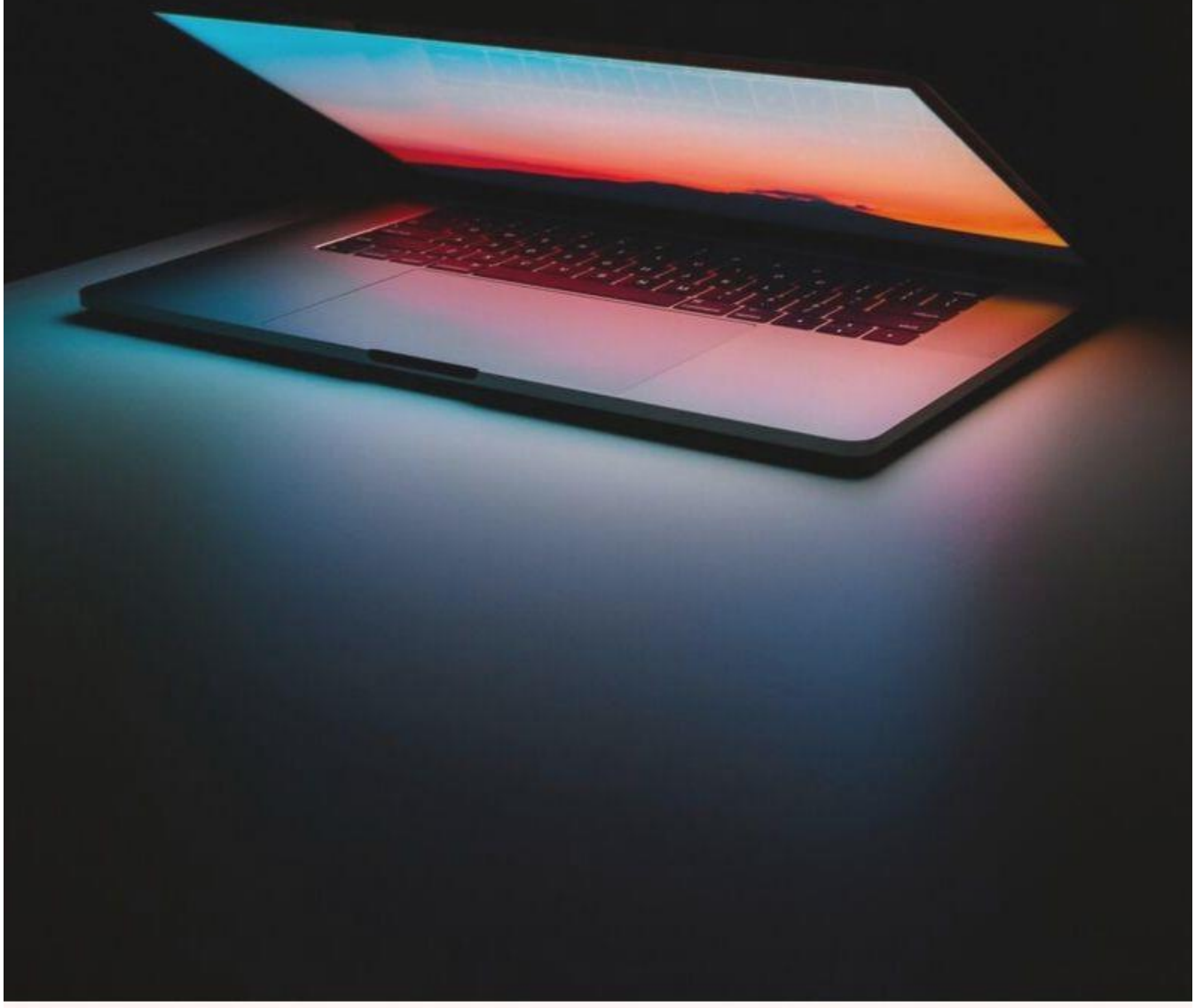
BEWARE !

A GUIDE TO STAYING SAFE ONLINE



Beware!

Co-funded by the
Erasmus+ Programme
of the European Union

BEWARE

Ersamus+ Programme Strategic Partnership

AGREEMENT No. **2018-1-RO01-KA205-048881**

Project Coordinated by:

Smart Educational Projects

Strada Calea Severinului, Nr.59, Bl.1, Ap1

TÂRGU JIU

Romania

https://www.bewareproject.eu/ https://www.facebook.com/bewareprojecteu/

https://twitter.com/eu_beware https://www.instagram.com/bewareproject/

https://www.linkedin.com/company/beware-project/

This project has been funded with support from the European Commission. This publication reflects the views of only the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Additional information on the Erasmus+ is available on the Internet via the Erasmus+ Project Results Platform https://ec.europa.eu/programmes/erasmus-plus/projects/

Project Partners:

acrosslimits

IFOM

Interactive 4D Serious Games Labs

younet

SEP

Preface

BEWARE is a project, designed to raise awareness among youths about potential dangers online, whilst equipping them with the knowledge and power to protect themselves. It aims to reach young people, youth workers and other EU citizens to become empowered and responsible digital users.

5 European Superheroes (otherwise known as Project Partners) have joined forces to execute a detailed set of project objectives set out to improve the knowledge and skills of specifically selected sidekicks (target groups).

This guide is the result of their research carried out in different countries and will be the sidekicks' bible. It covers 2 chapters:

- Data Protection in the Virtual Environment
- Cyber Bullying: from Game to Misdemeanour

Amongst other things, it will target the peer-to-peer part of online safety, which is increasingly fostering harassment and cyberbullying, as well as the growing threat of information and identity theft. In combination with it, an interactive game has been developed to enhance the acquired knowledge and skills.

This guide is especially dedicated to young people, so it was designed using informal teaching methods to make interaction and learning more enjoyable. A few hosts will accompany you, on your journey through the exciting world of virtual reality, a world that, on one hand is loads of fun while on the other hand could be a great source of danger!

So let's get to know our hosts:

Zoe – always online, does not want to miss anything that happens to her friends (all the time on Facebook or Instagarm), she is an avid online shopper; always ready to make mistakes online

Joe – the guy who has basic knowledge of the online environment. He doesn't have the patience to read too many details, but he still wants to be safe. He will give you some tips along the way.

Bob – the curious guy who will discover a lot of new things about the virtual world and will gladly share them with you.

Linda – our older friend, who always comes up with stories and questions to tickle our brains!

ACTIVITY FOR GROUPS

Index

Chapter 1

Data Protection in the Virtual Environment

1.1. Generic Introduction

Purpose of this Document

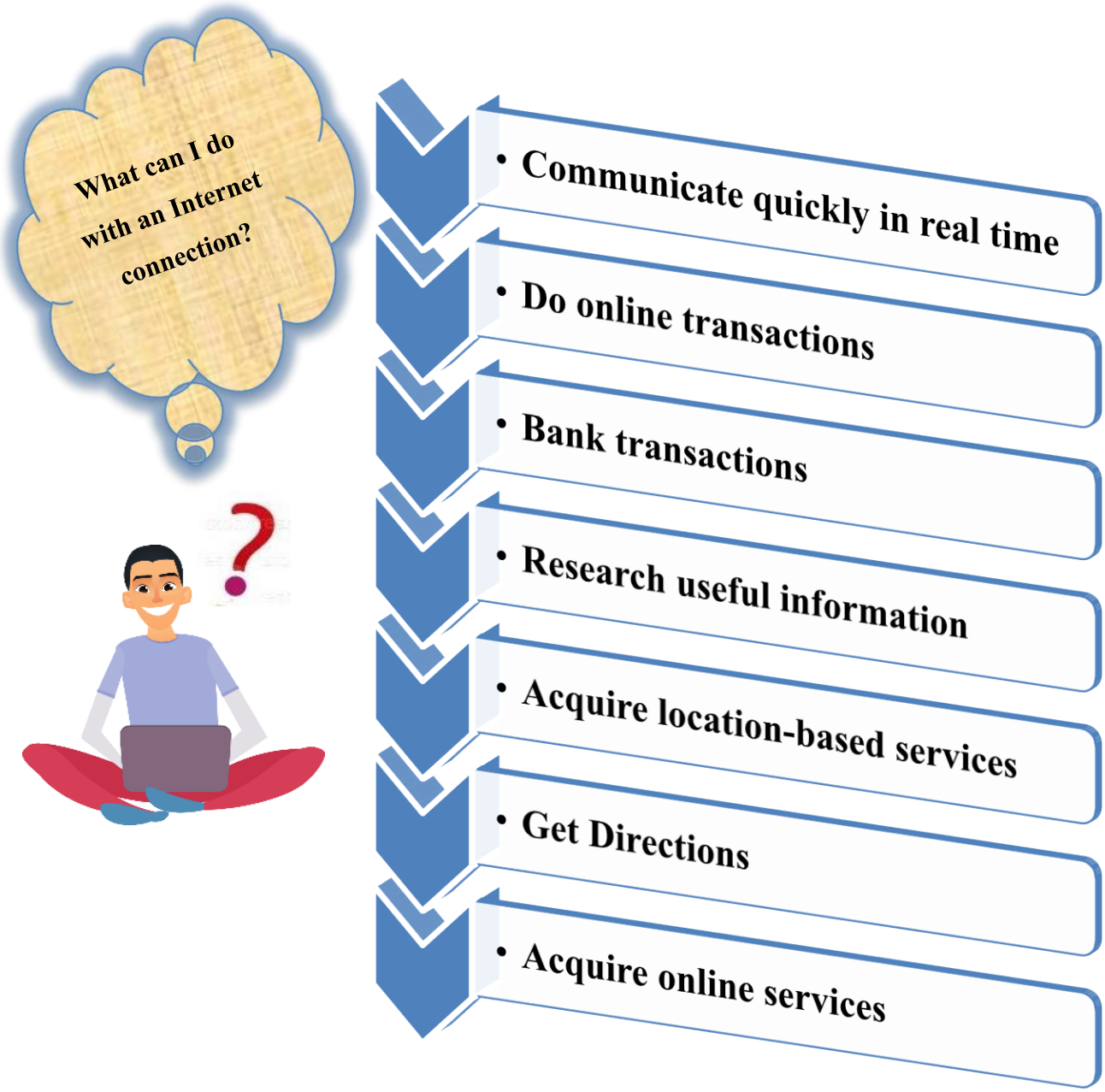
Our lives are predominantly being lived in parallel nowadays - in the real world, where we physically meet with family, friends and workmates, and at the same time online, where we interact with the same or different groups but in a completely different way to our "natural" style of socialization. As society becomes more technological and connected, the younger generations are more and more living a large part of their lives online - to play, to study and to work. However, our online 'lives' are not without peril - there are different and sometimes subtle dangers that could spring upon us if we are too 'naive'. Just like we tell children not to accept sweets from strangers or jump into a van with anyone they don't know, nowadays we need to teach them also how to protect themselves online.

This chapter aims to address these issues: How to be safe online, and how to protect ourselves and those we love from potential dangers. It is aimed at trainers, teachers and at the young people themselves and it is written in simple to understand language, with clear tips and ideas that can be implemented with ease. The team behind this publication is made up of experts, ICT companies, non-profit organizations, parents and the young people themselves. All these people have a common vision - to build a safer future for our loved ones.

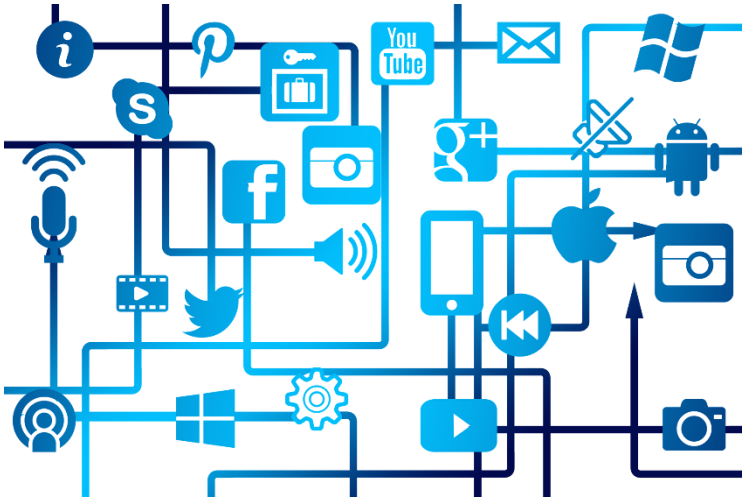
Setting the Scene

Since around the 1970's, the world has witnessed a technological revolution - a global paradigm shift in the way we communicate in our social relationship. New technology has impacted every aspect of our lives from early childhood to older ages. Some individuals argue that the Internet has revolutionized social interactions, where others argue that the Internet has already lead to loss of privacy, impersonal communications and even isolation.

Nowadays, everyone uses a device that is connected to the internet like a smartphone, tablet, pc, laptop etc. The truth is that internet connectivity makes everyone's life much easier and everyone loves it ….



Overall the internet has made life much more comfortable and efficient for all of us using it. However, there is another side to this story. Whenever you are online, your device is transmitting data over the internet, data exposing your personal details like your name, your location, your topics of research, the applications you are using, etc.

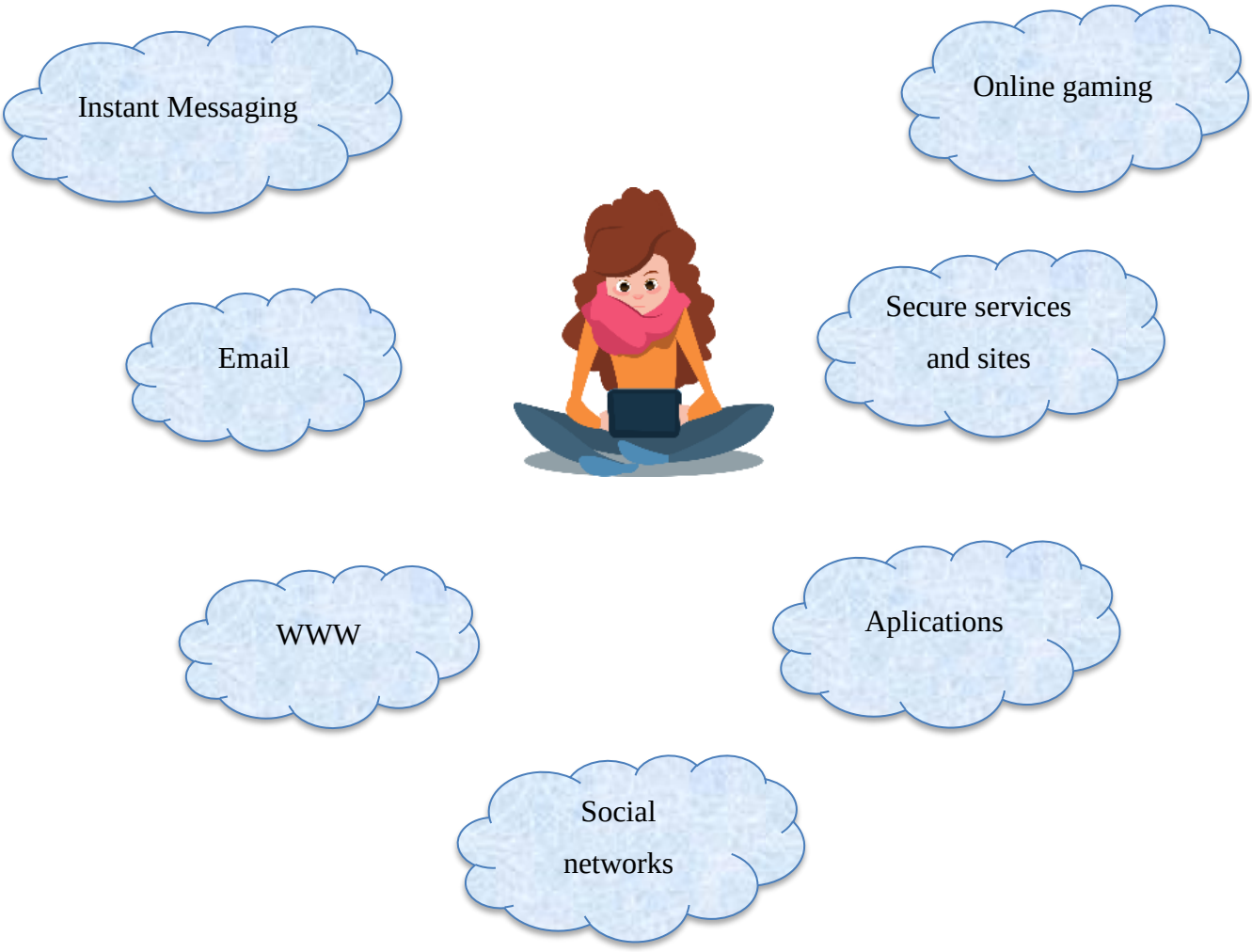


For this reason, it is essential especially for young people to understand the meaning and importance of "Data Protection in the Virtual Environment". This guide will help you understand the risks of being online and will also pinpoint the safeguarding mechanisms you can use to prevent any form of cyber-attacks on yourself and others surrounding you.

1.2. Internet Security

The ‘Internet’ is nowadays a collective term that encompasses a variety of services that are all done and consumed online. Most people refer to it as the “web” - that is the actual sites that one can see through an internet browser as the internet, but really and truly the internet itself is the network that is made up of many more things than that.

The following is a non-exhaustive list of "Internet services”:



All the above services are based on online communications - between computers, servers and people. As such when we talk about internet security we refer to making sure that every party in these communications is safe and that the data that is passed remains also secure / intact.

Cybersecurity (internet security) has become an important consideration in all aspects of these communications and we cannot always assume that things will be ok. We must remain vigilant and careful of our actions (that sometimes are inadvertently done).

1.2.1. What could possibly go wrong?

- **WWW** - Websites can be hacked by people with malicious intent (or having nothing better to do with their time) and information can be changed from what the original authors wanted.

- **Email** - Unwanted email messages (SPAM) litter everyone's inboxes around the world. The unproductive time that this causes around the world is an economic disaster on a regular basis

- **Instant Messaging** - Harassment and bullying can be done via instant messaging to different people from 'unknown' friends or else from someone who has gained illegal access to other people's accounts.

- **Social Networks** - Oversharing, cyber-bullying, addiction to the 5 seconds of fame are all effects that could happen on social networks. 'Friends' online, are not necessarily real friends. Fake news is a phenomenon that is also used to 'brainwash' people into making choices in their lives, like who to vote for.

- **FTP** - Illegal files (copyrighted materials like movies, software) can be placed on underground FTP sites for people to download them. By participating in this, one is actually an ancillary to theft.

- **Secure Services and Sites** - Online theft can happen even from the more secure websites - like banks, governmental agencies and industrial/commercial entities.

- **Apps** - Some apps could have malicious intent to track or take data from your mobile phones. One should also be careful from apps that appear free but in reality, require people to enter their credit card details for 'additional features'.

- **Online Gaming** - Violent and realistic games could incite hatred or violent behaviour in persons who are more susceptible to mental manipulation, especially children and teens. Educators have remarked various times that students playing such games have violent traits with respect to other peers.

Online Gambling - Gambling games, online casinos and other such apps could lead to gaming addiction, hence jeopardizing the financial situation and general life situation of the gamers.

Your accounts have not been attacked. Are you sure? Let's see...

Through haveibeenpwned.com you can see circumstances in which your ID/email address has fallen into the hands of hackers or was made publicly available.

Enter on haveibeenpwned.com, type the ID or email address you usually use and prepare to be amazed! If your email address is old or if you have spent a lot of time online over the last few years, there is a high probability that it is on a list of accounts that have fallen into the hands of hackers

Hmm…. If I used the same password on all my accounts, someone could have accessed all the information I've posted online!!!

1.3. Data Protection with Passwords and Backups

Your data is the most important asset that you hold on the internet. Your data could be anything related to your personal life (photos, details of relatives), your school/work (assignments, reports) and your finances (banking, credit card details) etc. Only you and people you trust should have access to your data and no one should be able to modify it, share it and make it their own without your specific consent.

Always protect your devices (computers, mobiles, tablets) and your logins with a password. Passwords should be made safe and complicated, so they cannot be guessed by other people. Never save your list of passwords on your laptop, PC or mobile phone. Save them on a piece of paper or in your personal diary, where no one can access them.

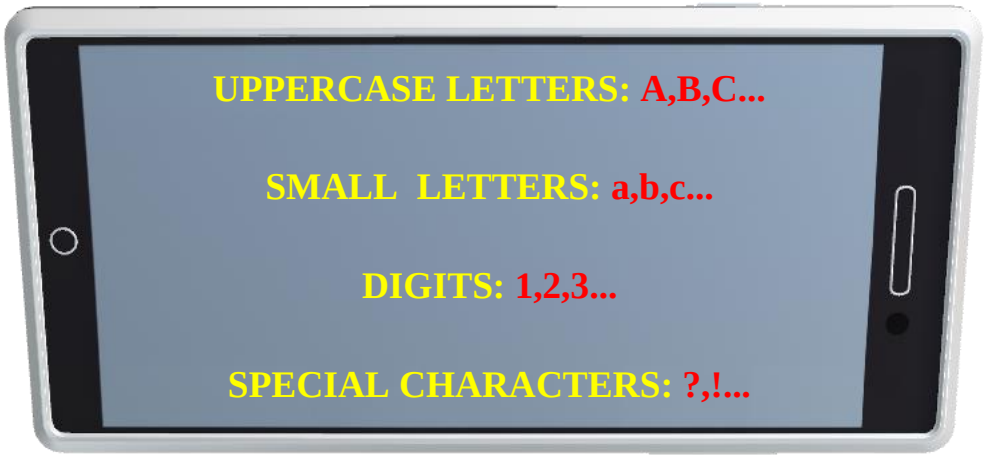
Change your passwords regularly for example every 3 months and do not use the same password for different applications. You must never share your passwords with anyone else, not even your partner, your family members or your best friends.

The following should never be used as passwords:

- Your name/surname/date of birth
- Names or date of birth of your best friends, family or pets

Your password is ... .. **love?** (nice ... no?). **This password can be broken by a hacker in ... 1 second** (according to Kaspersky Secure).

1.3.1. What should a Powerful Password Contain?



Minimum number of characters: 8

Recommended: 12-14

Everyone will surely agree that **kdB25?as!_S87A** is a very powerful password. Creating a strong password based on the above criteria is not complicated. The problem is..... memorizing it!!! And that would not be such a difficult problem if it were only one single password ...

TIP: to create an easy-to-remember password system, you create a root that you can use for all your accounts/applications. For each account you will add 1 or more characters, using an algorithm known to you only.

Here's how I did it:

- *my root:* **Freetime?2018**.
- *my algorithm: add the first letter of the app name at the beginning of the root and the last one at the end.*
- *My passwords will be:*
  - ***Yahoo:*****YFreetime?2018O**
  - *Facebook:***FFreetime?2018K**
  - *Instagram:* **IFreetime?2018?M**

This is just a simple example. It is important to be creative, to keep in mind the rules of conceiving a strong password, and to set up an algorithm that only you know and understand! Once you've created your password, check with an antivirus program that offers this feature. Kaspersky Secure Password Check shows how long it takes to break your password.

Verify the password
with Password Check

APPLICATION: Create a root that meets the above criteria and an algorithm that you can use for your password

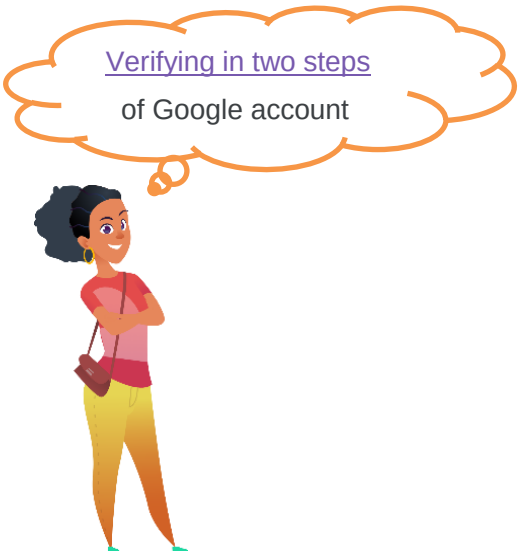
If you do not trust that you can generate a strong password yourself, use one of many available password generating sites: **PWGen**, **LastPass**, **Intuitive Password**, etc. The problem is that you will not be able to remember all of these passwords, and you will have to turn to application password managers, which store data in a secure and encrypted storage that can be accessed using a single master-pass (for example: LastPass, Dashlane, Kaspersky).

APPLICATION: Go to one of the sites above and create an account.

Authentication in 2 steps. A password can be stolen via phishing or you can divulge it yourself willingly or by mistake. A more secure way is 2-step authentication. This feature is present in almost all major online companies. The basic principle is the following:

- If you access your account on an unknown device, after entering the correct password, you must pass an additional check.
- Verification is done with a code received via SMS or e-mail.

So even if your password has been compromised, the attacker will not be able to access your account without having access to your device**:** phone, email.



APPLICATION: Verify that you have 2-Step Authentication on your accounts. Enter this feature for at least one of your accounts.

The above tips do not guarantee 100% protection. A person skilled in security matters will be able to break your accounts. The good part is that individuals capable of such a thing are not so many or so preoccupied with you that they choose you as a victim.

The simple security measures presented protect you against a large number of individuals who are not hacking experts, but take advantage of the fact that you have chosen from the start to have a very low level of security. Some apps give you the option to save your password when you sign in. **This should be avoided all the time.**

You should back up your data regularly if the device fails and loses all your data. Backups should be encrypted with a password where possible and kept in a location separate from the usual place of living / work. At this time, you may also have online backup services that are safe and secure in a country other than your own, however, take care of what passwords you have configured to access such backups.

PRACTICAL APPLICATION FOR GROUP ACTIVITY 1

1.3.2. Protecting Personal Data in the Online Environment

You should never make your personal data public on the online environment as other people can get access to that data and use it in a malicious way. Personal data can include any of the following:

- Contact details
- Health Records
- Financial Information
- School / Education records / certificates
- Employment History
- Location details (where you are physically at the moment)
- Family relations and friends' details
- Photos / videos / recordings

All of the above data is precious, some of it we 'give away' on a regular basis even to people we do not know - like our name and where we live, however we need to be more careful online since people might not be who they say they are.

Let's not forget!

Personal data or ethnic or racial origin, sexual orientation, health or political opinions are considered sensitive data and, according to RGPD, can only be used following explicit user consent.

What are the special categories of personal data?

- race
- ethnicity
- religion
- health data
- trade union membership
- philosophical or similar beliefs
- Sexual life data
- political orientation

In addition, data with a special regime are considered:

• Personal data having a general applicability identification function such as Personal Number (CNP)

• personal data relating to criminal offenses or contraventions

With the new European GDPR law, our personal data is better protected, and even if in the past we have given consent for others to have it, we can now actually revoke that permission and they have to 'forget us' and remove all the copies they have of our data. This is actually a legal obligation that anyone in the European Union has to abide by. The aim of the GDPR is to protect all EU citizens from privacy and data breaches in today's data-driven world. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies; the key points of the GDPR as well as information on the impacts it will have on business can be found below.

- **Increased Territorial Scope (extraterritorial applicability) -** it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location.
- **Penalties -** Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater).
- **Consent** - companies are no longer able to use long illegible terms and conditions full of legalese. The request for consent must be given in an intelligible and easily accessible form, using clear and plain language. It must also state the purpose for data processing.

As users (data subjects), the GDPR regulation gives us the following rights:

- **Breach Notification -** breach notifications are now mandatory within 72 hours of awareness in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". Data processors are also required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

- **Right to Access -** data subjects may obtain confirmation from the data controller as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format.
- **Right to be Forgotten -** Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.
- **Data Portability -** GDPR introduces data portability – the right for a data subject to receive the personal data concerning them – which they have previously provided in a 'commonly use and machine-readable format' and have the right to transmit that data to another controller.
- **Privacy by Design -** calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically, controllers should hold and process only the data absolutely necessary for the completion of their duties (data minimisation), as well as limit the access to personal data to those needing to act out the processing.
- **Data Protection Officers -** DPO appointment is mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. They have to follow a list of defined internal record keeping requirements.

PRACTICAL APPLICATION FOR GROUP ACTIVITY2

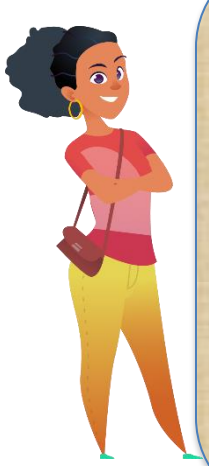
1.3.3. Protecting yourself whilst Shopping Online

SCENARIO 1

Because she has a short break between 2 lectures and many assignments to finish, Amy decided to work in a pub to earn some time. As she needs an internet connection, she logs in using the pub´s Wi-Fi. An e mail from a cosmetics site, reminds her that she had to order a perfume for her mother and something for herself. She logs into the site and makes the purchases online. Meanwhile, some friends appear at a nearby table. Amy needs a coffee, so she goes to the bar and leaves her laptop open on the table. She is just at 2-3 steps away ... Two days later, her friend Carla sends her an upsetting email after she received a picture of Amy with her ex-boyfriend! That picture was taken a week before at the mall and was saved in the "funny picture" folder on Amy's laptop. Maybe Amy was a little bit too negligent with her laptop ... Maybe she made other mistakes too ....

Do you know what mistakes Amy did?

And why couldn't I do that when I go to the toilet or to the bar?



SCENARIO 2

Sue was on a trip with her friends and her mobile data traffic allowance was used up, so she had no internet access. Her best friend called to inform her that her favourite fancy clothes' site had a huge online sale for the next 2 hours only. Sue couldn't miss such an opportunity, she had to find a solution ... She asked one of the guys she was travelling with to provide her a hotspot through his own mobile! Greg accepted to help her, and Sue happily managed to purchase 2 beautiful dresses she had dreamed about for a long time. She bought them using a credit card ... A few days later, she noticed that there were some transactions on her credit card that she didn't make herself….

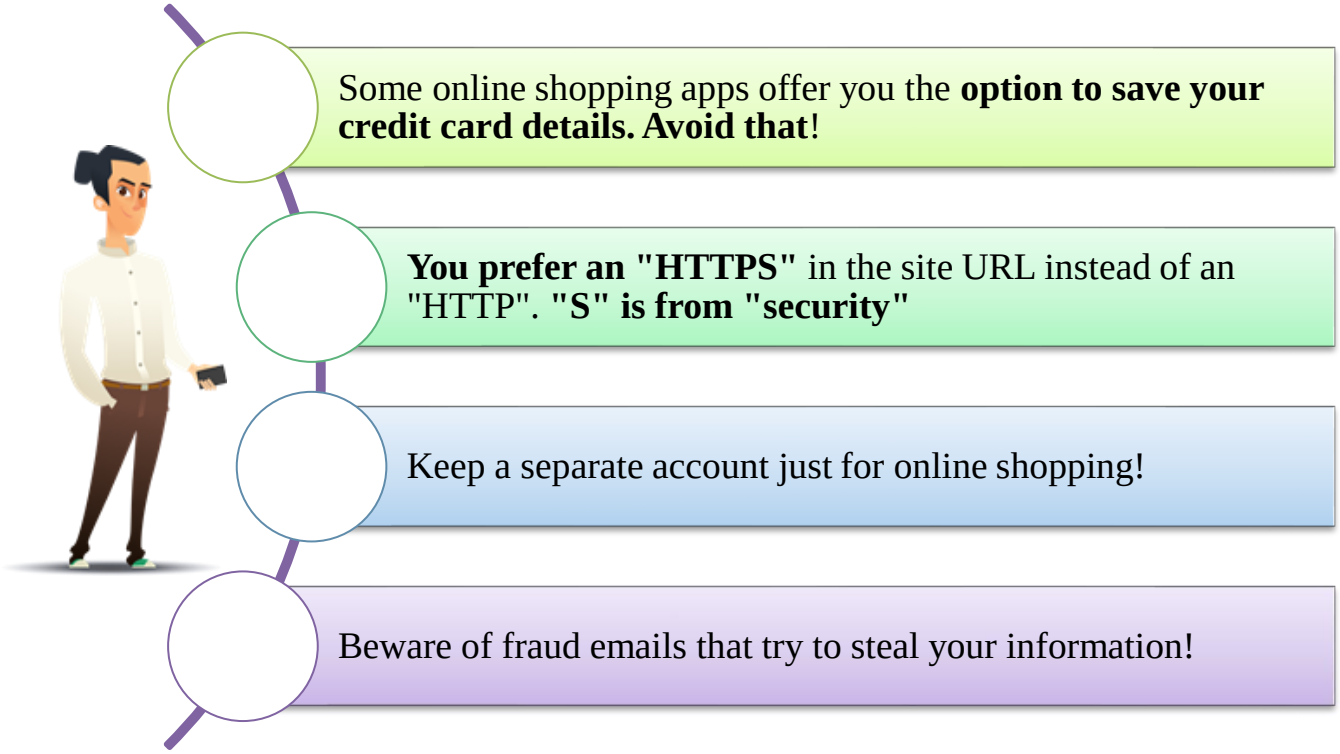
That's exactly what happened to me! But unfortunately I don´t know why ...

Did you know?

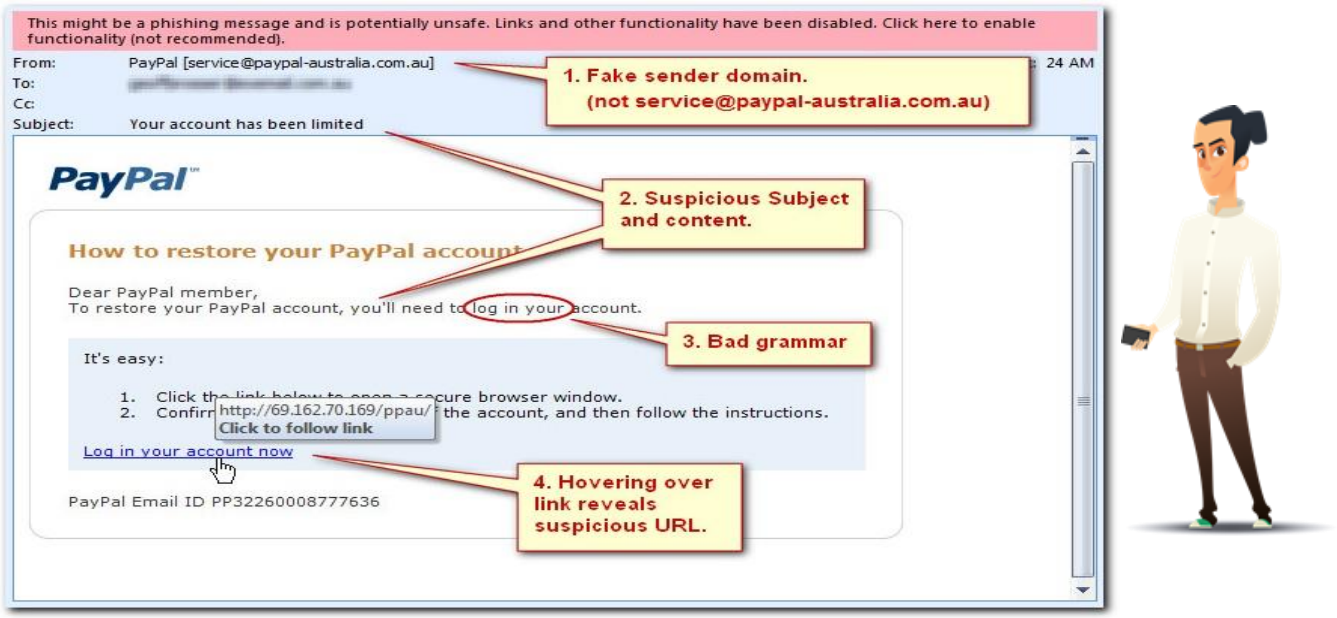
When you use someone else's device as a hotspot to connect to WiFi, this device can record all the data you send, including passwords and credit card details!!

- Do not shop online when you connect via a hotspot!
- Do not leave your computer open in public areas! Someone might access your files without a password.
- Put an automatic / sleep time and make sure a password is required after the computer wakes up

PRACTICAL APPLICATION FOR GROUPS 3



Here's an example of phishing fraud email



Protect yourself while you are online

On an online registration form do I have to fill in all my personal data?

If you are filling a form and your personal details (address, mobile number, etc) are not compulsory (not marked with *), do not provide them

What do I do if I want to get rid of spam mail?

Create another email address you only use for online shopping!

Keep your personal email address only for official and reliable communications as much as possible!

Do not automatically fill in everything on a form!

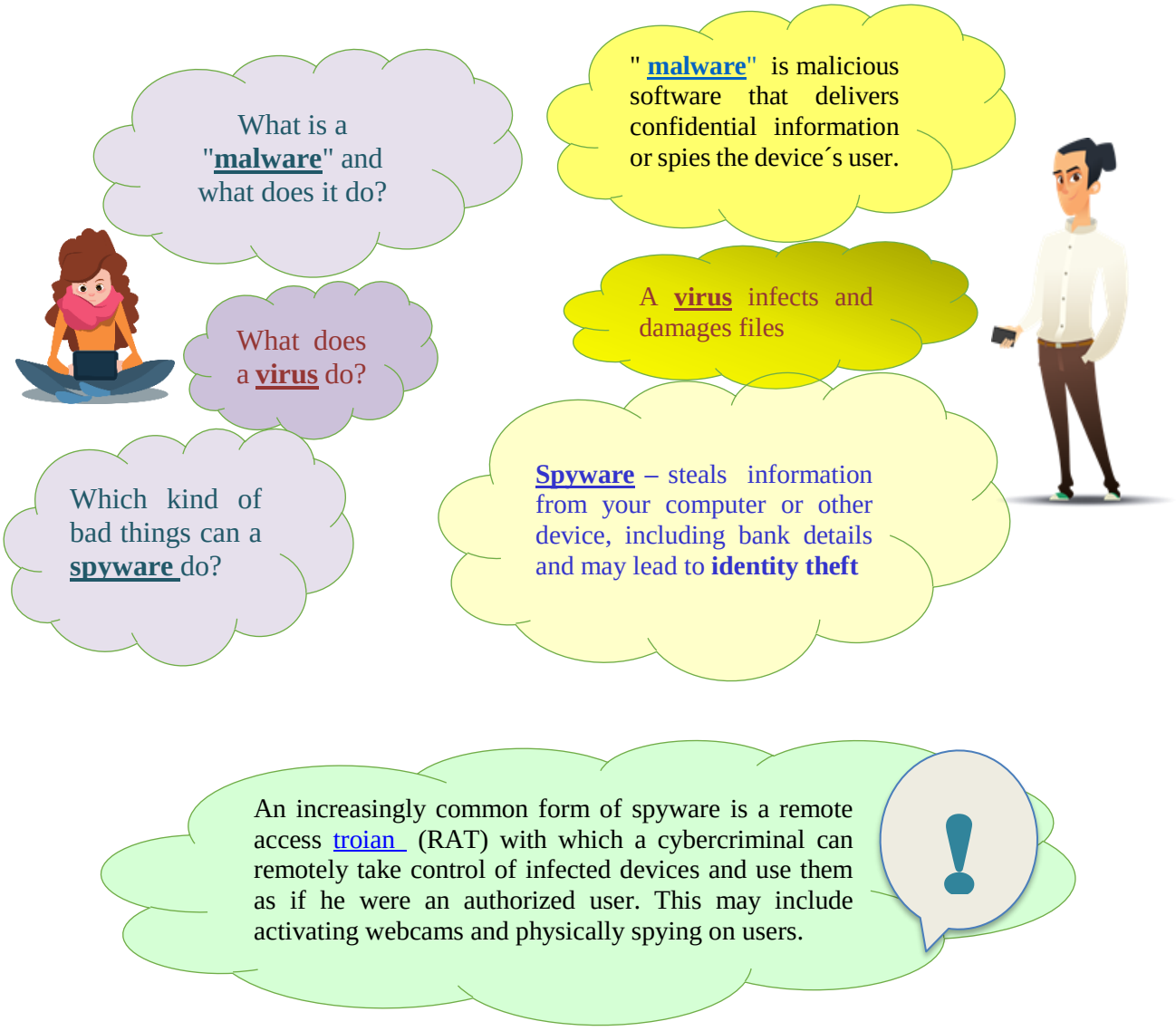
Some confirmations may mean agreeing to receive spam or selling your data to 3rd parties

Can I get rid of the unwanted ads that appear when I access a site?

Yes, install Adblock on your phone or laptop

1.4. Protecting Your Computer/Laptop

- Make sure you always have the latest software / operating system installed since the new versions might have closed off some previously found bus / backdoors. Switch on the automatic updates so that you do not forget to do them manually
- Do not install software that has been downloaded from pirated websites / other illegal sites since these could have been modified to be harmful
- It is essential to keep your Internet security updates (software antivirus , anti- malware)) to provide the most complete protection



Does an antivirus protect me from any unpleasant situation on the internet?

Security software **does not protect you** against: **Spam,** fraud, or other online malware activity that is not initiated by **malware**

- Do not open any file attached to an email from an unknown source
- connected USB devices (such as memory sticks, external hard drives, MP3 players) are very common carriers of viruses.
- CDs / DVDs can also contain viruses.
- Do not open any file from web distribution companies such as HighTail (formerly YouSendIt) or Dropbox, which have been uploaded from an unknown source
- Enable macro protection in Microsoft Office applications such as Word and Excel.

SCENARIO

Jim has a technical problem with his laptop has no clue on how to solve it. One way or another, he must finish the assignment for tomorrow! His friend Tom, a computer expert, is out of town, but he offers to help Jim remotely if he installs "TeamViewer". Jim promptly installs it, and within an hour Tom fixed his problem so Jim could finish his work .... A few days later, during a class presentation, Jim realises that Tom's assignment about "History of the Mediterranean" is an exact copy of his own presentation that he had worked on for a good few weeks!! Had his "friend" done something else besides fixing his problem???

What is "Teamviewer?" Is it good or bad to use it?

TeamViewer is a remote desktop control software that can also be used for desktop sharing, online conferencing, and even file transfer between computers

TeamViewer makes it possible to provide **remote technical support.**

Avoid using TeamViewer or any other software that allows desktop sharing!

Destructive viruses and other programs can be installed on your computer without you realizing, like activating your webcam without you knowing it.

If you have already allowed access to your computer, the only way to make sure you remove anything installed without your permission is to format it!!!

1.5. Social Media Settings and Social Media Platforms

Social media is a collective term meaning all the types of online communication channels dedicated to community-based input, interaction, content-sharing and collaboration. Websites and applications dedicated to forums, microblogging, social networking, social bookmarking, social curation, and wikis are among the different types of social media. Here are the biggest examples of social media:

Facebook is a popular free social networking website that allows registered users to create profiles, upload photos and video, send messages and keep in touch with friends, family and colleagues. According to statistics from the Nielsen Group, Internet users spend more time on Facebook than any other website.

Twitter is a free microblogging service that allows registered members to broadcast short posts called tweets. Twitter members can broadcast tweets and follow other users' tweets by using multiple platforms and devices.

Google+ (pronounced Google plus) is Google's social networking project, designed to replicate the way people interact offline more closely than is the case in other social networking services. The project's slogan is "Real-life sharing rethought for the web."

Wikipedia is a free, open content online encyclopaedia created through the collaborative effort of a community of users known as Wikipedians. Anyone registered on the site can create an article for publication; registration is not required to edit articles. Wikipedia was founded in January of 2001.

Pinterest is a social curation website for sharing and categorizing images found online. Pinterest requires brief descriptions, but the main focus of the site is visual. Clicking on an image will take you to the original source, so, for example, if you click on a picture of a pair of shoes, you might be taken to a site where you can purchase them. An image of blueberry

pancakes might take you to the recipe; a picture of a whimsical birdhouse might take you to the instructions on how to build it.

LinkedIn is a social network site specifically designed for career and business professionals to connect. The goal of the site is to allow registered members to establish and document networks of people they know and trust professionally. Over 550 million professionals use LinkedIn to cultivate their careers and businesses. Unlike other social networks in which you might become "friends" with anyone and everyone, LinkedIn is about building strategic relationships.

Snapchat is a mobile app for Android and iOS devices. One of the core concepts of the app is that any picture or video or message you send - by default - is made available to the receiver for only a short time before it becomes inaccessible. This temporary nature of the app was originally designed to encourage a more natural flow of interaction.

1.5.1. Aggression Methods in Social Networks

Fraping or identity substitution describes the situation when someone logs into a young person's social media account and posts on them information with "impact" on users. These seemingly innocent jokes can cause a lot of suffering, especially for a more sensitive person or at a difficult time in his life. Let's not forget that the information "released" in the online environment can no longer be deleted.

False profiles are specifically designed to mislead and humiliate or attack the victim in any way. Or it may happen that someone is stealing the online identity of a young person using personal data, photos, address, contact details and using them for another profile with the intention of hiding their own identity, believing they will not be discovered.

Trolling is also a form of cyberbullying, in which the attacker tries to obtain a reaction from the victim through aggressive language or insult. The aim is to find victims, especially vulnerable people, to aggrieve them by taking advantage of a certain circumstance.

Doxing is the Internet-based practice of researching and broadcasting private or identifiable information (especially personally identifiable information) about an individual or organization. The methods employed to acquire this information include searching publicly available databases and social media websites (like Facebook), hacking, and social engineering. Be

careful with the information about you, but also about the information about your friends or family.

Elicitation is the strategic use of conversations to get information without the victim realizing that he is subjected to a real interrogation. Be aware of these tactics, be careful what you answer to certain seemingly innocent questions, what you say about yourself, your family and friends.

1.5.2. What could possibly go wrong?

Problems on social media can be categorized by the following groupings:

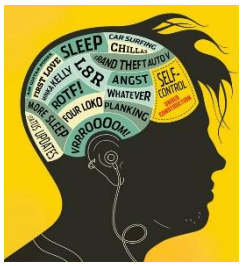
Children and youths are mostly vulnerable to this kind of Online Risks. This is because of their curious nature and need to explore, develop their image and character, belong in a group, etc.. Because of their young age and lack of experience, they are not always fully aware of the consequences to their behaviour.

Europol has been running a campaign against online sexual coercion and extorsion. Following is the official page for this public awareness and prevention campaign. It contains also a video in various EU languages:

https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime

Why does this happen?

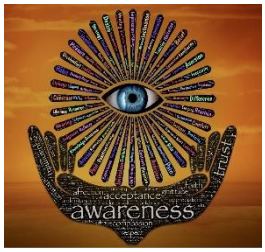
Cyberpsychology, also known as Internet psychology or web psychology is the study of the human mind and behavior and how the culture of technology, specifically, virtual reality, and social media affect them. Mainstream research studies focus on the effect of the Internet and cyberspace on the psychology of individuals and groups. Some hot topics include: online identity, online relationships, personality types in cyberspace, transference to computers, addiction to computers and Internet, regressive behavior in cyberspace and online gender-switching.



Such studies show that human beings tend to behave differently in real life than they do when sitting behind a screen, especially if they are covering themselves through a fake or anonymous profile. The following effects are highlighted:

Online disinhibition effect (acting drunk)	Online escalation
• Illusion of being safer online • Open Playground: with children exposing themselves • Perceived lack of authority, the anonymity, as well as the sense of distance or physical removal	• Online behaviour is amplified • Easy to post negative feedback like offensive or aggressive text, especially if anonymous

Teenagers and youths may be easily subject to such behaviour because of their need to establish their unique identity. Nowadays, getting feedback from social media connections is the most common way for youths to eventually figure out who they are and what the world expects from them. This is because the first part of the teenage brain to develop is the emotional, impulsive limbic system. The rational prefrontal cortex will not get involved until the early or mid-20's. Hence in the period between teenage and early adulthood, youths have a strong need for attachment and belonging into peer groups. This is why they give such extensive importance to social networking. Such feedback may affect both positively and negatively the way teenagers develop their self-esteem, personal and sexual identity via peer pressure.



1.5.3. Offline Persona VS Online Persona

Research shows that people have 2 identities: the real/offline and the virtual/cyber/online. The cyber self is always under construction, psychologically and digitally.

Even while the real you in sleeping, the cyber you continue to exist. It is 'always on' - evolving, updating, making friends, making connections, gaining followers, getting "likes" and being tagged.

This can create a feeling of urgency, a continuous feedback loop, a sense of needing to invest more and more time to keep the virtual self current, relevant, and popular. In some cases, the cyber you shows a totally different image of the real you!

Problems that may arise when using social networks

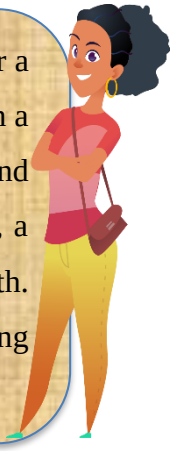
- **The online disinhibition effect**
- **Isolation and reduction of the desire to socialize in real environment**
- **The FOMO phenomenon**
- **Illusion of another identity**
- **Disturbances of the sleep routine**

APPLICATION – ***Answer Linda's questions and remember to be honest with yourself!!***

1. Do you think the experiences that you live in the on-ine environment influence your life? In what way? Try to note a few thoughts about it!
2. Do you know a concrete case, where something that happened in the online environment, has caused unpleasant consequences to somebody you know? Please write a few sentences about it!
3. Can you describe a recent online situation that has created you a sensation of wellbeing?

1.5.4. Providing Information and Images that may compromise your Identity

I want to propose **a game called "Be my spy!"** to you**.** Zoe and Joe will work together for a week. Zoe will post a lot of uncensored information without filterted images or thoughts on a social network (like she usually does). Joe will note and analyse everything he has seen and will interpret the information released online. Joe can play the role of a future employer, a journalist, a director of an educational institution who wants to offer a scholarship to a youth. At the end of the experience, Joe will share his own conclusions about Zoe, offering suggestions.



- Do not accept to do anything sexual
- Never make your personal profile public on Social media
- Do not give too many details about yourself on social media (ex. Your home address, your school, where you are at every hour of the day, etc..)
- Do not accept friend requests from people you don't know in real life
- Do not share indecent photos of yourself over social media or chat engines
- If you are being blackmailed over the internet, you should refuse to pay any kind of ransom and report to the police
- If someone you don't know asks you to meet in person, do not accept

1.5.5. Fake Followers, Fake Profiles and Fake Apps

Fake Profiles and Applications are a reality that is common since the onset of social media. People setting up fake profiles might have different purposes for doing so. Some are simply malicious while others have criminal intents. Europol has been running a prevention and public awareness campaign called "Don't F***(ake) up!".

https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/be-aware-of-fake-social-media-accounts-and-fake-mobile-apps

Following are the main highlights of this campaign:

Fake social media accounts

On social media, counterfeiters can:

- Register fake profiles and pages containing the original brand name.
- Offer for sale counterfeit products through their accounts, pages or in groups.
- Advertise their fake products through social media ads, luring you to their illicit websites with flash sales for items that turn out to be fakes.
- Tag their fake products with luxury brand names so that they appear in your searches.

Detecting fake social media accounts can be tricky, even for law enforcement authorities. Check some basic F***(ake) Up signs!

- If there are many updates and content published but little conversations and engaging with members.
- If you receive a request to wire money or reveal sensitive information. A tactic used by scammers.
- If it pushes spam, shares the same link repeatedly in a short period of time or provides misleading information about the destination of a link.

- If it doesn't have the verification indicator as a high-profile user. Consult the social media platform's FAQs or user guidelines to familiarize yourself with their indicators

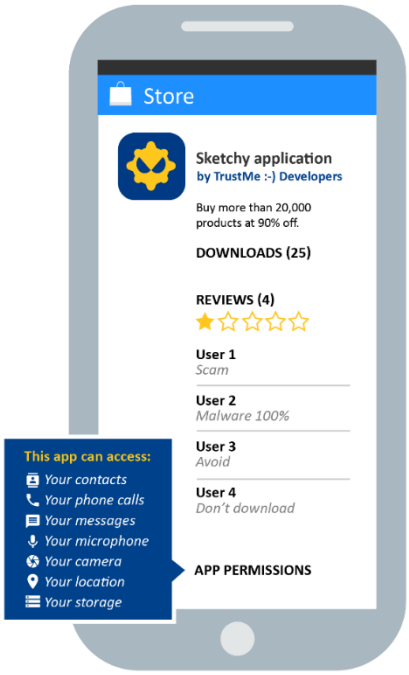
Fake Mobile Apps

With apps becoming more popular as a way to shop, be aware of fake apps exploited by counterfeiters! Just because an app is in the Official App Store it doesn't mean that it is a legitimate app!

- Fake apps might use original trademarks
- Fake apps may redirect customers to illegitimate websites with the purpose of stealing personal and financial information.
- Fake apps will pose as security updates, and clicking on the links may also lead to your information being stolen.
- If you receive an unexpected SMS, a strange alert or notification, or unusual requests from what may seem to be your bank or other familiar brand, beware: criminals may be trying to rip you off.
- Be cautious of links you receive in email and text messages that might trick you into installing apps from third party or unknown sources.

Before downloading an app, Check the F***(ake) Up signs!

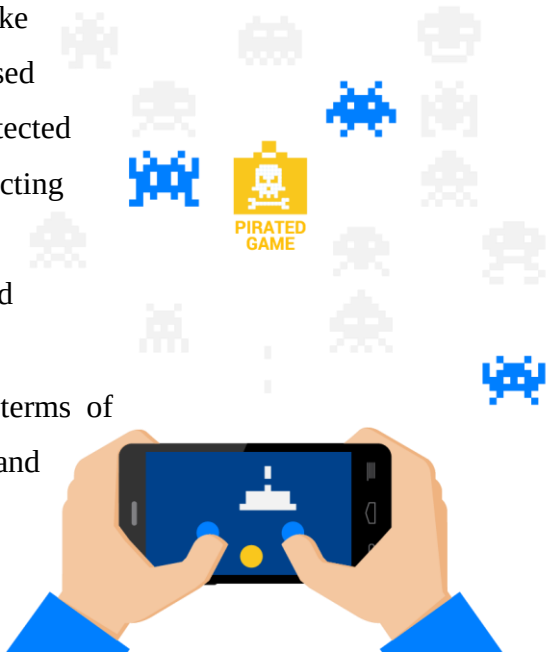
- Be suspicious of apps that promise very high shopping discounts.
- Check the publisher of the app. Criminals can use similar names; so be careful.
- Check other user's reviews and ratings. A fake app will likely have zero reviews while a real app will likely have thousands.
- Check the publish date. A fake app will have a recent publish date, while a real one will have an "updated on" date.



- Check how many times the app has been downloaded.
- Look for spelling mistakes in the title or description. Take extra caution if it looks like the language isn't the developers' first language.
- Read the app's permissions. Check which types of data the app can access, and if it might share your information with external parties. Does it need all these permissions? If not, don't download it.
- When in doubt, visit the official website of the brand or seller and look for the icon or button that reads "Get our app".

Fake game apps and pirated video games

- Be aware about threats associated with fake (pirated) video game apps and unauthorised copying or distribution of copyright protected software. Instead of having fun, you risk infecting your device with computer viruses, since most of the cracks are poorly disguised malware.



- IP infringers exploit opportunities both in terms of counterfeiting physical gaming products and illegally offering content on-line.
- Counterfeit consoles can pose a serious risk to your health and safety

- Fake game apps and pirated video games can harm your computers and mobile devices by installing embedded malicious viruses.

1.6. Annex 1 –Practical Applications and Activities for Youth Workers

PRACTICAL APPLICATION FOR GROUP ACTIVITIES 1

1. Ask participants to come up with ideas of creating strong passwords.
2. What methods do they normally use to create their passwords?
3. Allow time for an open discussion between the group members.
4. Moderate the discussion to be a constructive session.

PRACTICAL APPLICATION FOR GROUP ACTIVITIES 2

1. Ask participants to give examples of personal information they have personally posted online (contact details, school results, study certificates, medical test results).
2. Create groups of 3 people and ask the participants to analyze the team members' profile and posts for 10 minutes, to write down their findings, then each participant will analyze any mistakes made.

PRACTICAL APPLICATION FOR GROUP ACTIVITIES 3

1. Ask participants to identify mistakes made by Amy and Sue.
2. Let the participants discuss openly their opinion about what they think are mistakes or not.

Ice breaking activity to introduce the participants and get to know them

Option 1: Introduce me!

Situation: This game is appropriate at the beginning of the group activity to replace the classical round of introductions of the participants.

Goal: Lifting the barriers caused by the new environment and the unknown partners, memorizing the names and creating a relaxed atmosphere from the beginning.

Description: Split the group in pairs, where the 2 partners are unknown to each other. The partners intoduce themselves and ask some personal questions to get to know each other. (example: How old are you? Where are you from? Which school do you go to? What are your hobbies? etc.) The task is for the pair to get to know as much as possible about each other in the allocated time. In a next step, everyone joins up in a large circle and a leader calls one pair at a time to go to the middle. The partners forming a pair must describe each other.

Recommended number of participants:10-20 persons

Ideal location: Indoor space, but it can also be done outdoors

Necessary time: Partner to partner introduction: 3-4 minutes. Pairs to group introduction: 20-25 minutes (about 2 minutes for each pair)

Developed skills and key competences: - Ability to adapt - Communication in the mother tongue - Tolerance - Assertiveness - Interpersonal and social competences - Initiative - Memory capacity - Ability to get information and filter – Active Listening – Concentration - Attention - Self-knowledge - Self-criticism - Presentation skills – Public Speaking

Special attention: Sometimes, young people find it difficult to come out and speak about themselves in front of an audience especially if they have difficult backgrounds like poor or rural origins, financial difficulties, broken families, family problems, lack of education, etc... Through the game, sharing of personal information is facilitated with only one person, rather than with the whole group. The game also offers a self-awareness opportunity to the participants who will see themselves in the mirror through the eyes of their partners.

Ice breaking activity to introduce the participants and get to know them

Option 2: Present yourself using the extracted word!

Situation: This game is appropriate at the beginning of the group activity, replacing the presentation game.

Goal: Lifting the barriers caused by the new environment and the unknown partners, memorizing the names and creating a relaxed atmosphere from the beginning.

Description: Each member of the group receives a small piece of paper, on which s/he must write one word. The papers will be folded and placed in a box. Each participant takes a random note and then s/he must intorduce him/herself using the word on the note, in each sentence.

Recommended number of participants:15-25 persons

Ideal location: Indoor space, but it can also be done outdoors

Necessary time: 1-2 minutes to write the words and collect the notes
15-20 minutes for intorudctions (1-2 minutes/person)

Required equipment: small pieces of papers, ballpens, box

Developed skills & key competences:

- communication in the native language
- ability to express oneself
- creativity
- sense of humor
- information processing and rapid response
- tolerance
- memory development

Special attention:

• Define the time allocated to each participant's introduction and respect it!

• Manage any situation that may hinder a participant’s introduction

• Create a pleasant, team-friendly atmosphere for everyone to feel special/important and bring something new to the group.

SUGGESTED ACTIVITY FOR YOUTH WORKERS 1

The Devil's Advocate – *non-formal method*

Theme: What password do I protect my accounts with?

Situation: This method is recommended to identify the pros and cons of different types of passwords that may be used for different accounts:

- Creating a password by using a root and an algorithm
- Using a dedicated password creation and storage site
- Using 2-step authentication

Description: The group will be divided into two parts:

- Group 1 will propose positive arguments for each of the 3 methods
- Group 2 will propose negative arguments for each of the 3 methods

The coordinator will draw a table with 2 columns on the flipchart or board: **Pros / Cons**

Once all points have been identified, the group will discuss, analyze and critisize constructively. Possibly, a common agreement on the best protection method is identified by the group.

Recommended number of participants: 10-20 youths

Ideal location: Closed space

Necessary time: about 30 minutes - 10 minutes to identify pros and cons, 20 minutes for analysis and discussion

Necessary equipment: sheets of paper, markers, flipchart, board

Evaluation aspects:

The evaluation consists of group discussion based on sharing of personal opinions with respect to pros and cons provided by the rest of the group. Constructive critisicm and goal-oriented attitude have a very important role in this game, and it is indispensable to remain within the limits of reality.

Developed skills:
- communication
- initiative spirit
- collaboration
- assertiveness
- presentation skills
- creativity
- collective thinking
- concentration capability
- active listening
- ability to express oneself
- logical thinking
- ability to associate
- Critical perspective

Special instructions: Do not judge the arguments of others and take advantage of controversial situations to lead the group members to think deeply about the argument and think outside of the box.

SUGGESTED ACTIVITY FOR YOUTH WORKERS 2

The World Café – *non-formal method*

Theme: Data Protection in the Virtual Environment

Situation: The method is recommended for debating Data Protection mechanisms and is based on the content of the entire chapter. The topics to be debated will be:

- Data protection with passwords and backups
- Personal data protection in the online environment
- Social Media Settings and Social Media Platforms

The goal of the method is to engage the participants into exchanging ideas and proposing creative solutions to raise awareness in youths to protect data in the virtual environment.

Description: The participants are split in groups of 4-5 people. Every group sits around a table debating 1 of the 3 topics while having coffee and refreshments. Each table will have a discussion topic and a youth worker acting as "host". These are fixed throughout the duration of the activity:

The host introduces the newcomers to the topics and moderates the discussion to ensure it's logical and constructive. After a first round of 20-30 minutes, groups move to the next table, where they will discuss another of the 3 topics, while the hosts remain at their assigned tables.

After each group has completed all three rounds, a final round of debating with the whole group can be organized to share the conclusions.

Now the BEWARE game will also be introduced!

Recommended number of participants: 12-30 divided in groups of 4-5

Ideal location : Ideally, the space for this acrtivity should be laid out as a café or eventually the activity should be held at a café. This aspect is very important because the relaxed atmosphere of a café will stimulate free thinking, creativity and involvement of all participants.

Necessary time:

Total of 2.5-3 hours split as follows:

- 30 minutes for each of the 3 topics.
- 1-1.5 hours for the final discussion round, where the participants will share their conclusions and play the game BEWARE!

Necessary equipment:

- flipchart paper on each table so that the hosts and guests can write down the ideas (us of notebooks not recommend, to keep the informal setting)
- colored markers and sticky notes
- refreshments (coffee, cookies, etc.)

Developed skills:
- communication
- initiative spirit
- collaboration
- assertiveness
- collective thinking
- active listening
- ability to express
- logical thinking
- ability to associate

Special instructions:

- Create a warm, welcoming ambience with comfortable chairs and relaxing musical background to put the participants at ease and unleash their creativity.
- The organizer should open the event with a detailed explanation of how the discussions will take place as probably many participants are not familiar with the format.
- Provide participants with the agenda of the working session and some promotional materials.

SUGGESTED ACTIVITY FOR YOUTH WORKERS 3

Poster / collage – *non-formal method*

Theme: Data Protection in the Virtual Environment

Situation: The method will be applied at the end of the training session on Data Protection in the Online Environment. The purpose of this activity is for the participants to express their opinions and ideas visually and to make it easier for the group to retain the most important aspects of

- Data protection with passwords and backups
- Personal data protection in the online environment
- Social Media Settings and Social Media Platforms

Description: Participants will be divided into 3 groups corresponding to the three themes. Each group will realise a collage / poster with visual representations of what they have learned on the topic assigned to them. The essence of the method is that the participants visualize the outcome of the taught content with respect to their own feelings and ideas. The "Creations" will be presented to the group by the members of each team. It is advisable to hold a discussion session at the end of each presentation.

Recommended number of participants: 15-20 persons divided in 3 groups

Ideal location: Closed space

Requiered time: 15-25 minutes

Necessary equipment:

- sheets of paper, colored paper sheets, old magazines
- colored pencils, pens
- scissors, glue
- other creative tools

Developed skills and key competences:

- communication in the mother language
- initiative spirit
- social and civic competences
- collaboration
- assertiveness
- ability to solve a problem
- creativity
- collective thinking
- concentration capability
- active listening

Special instructions:

- The youth workers should ensure that each member of the group is involved in teamwork. People who are not too active or creative must be motivated, while overly active / creative members should be led to allow space for others to express themselves.
- It is important for everyone to take part in making up the poster/collage to mount / draw something. The creation should reflect the ideas, identity and suggestions of everyone.
- If the group contains youths with lower opportunities (from disadvantaged groups), the activity will give them the opportunity to integrate in groups and help them valorise their ideas and self esteem.

1.7. References & Links:

https://www.europol.europa.eu/

https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides

https://cybersecurity.gov.mt/

https://www.welivesecurity.com/2017/09/28/android-lock-screen-pattern-isnt-safe-pin-code/

https://www.theverge.com/2016/5/2/11540962/iphone-samsung-fingerprint-duplicate-hack-security

https://arxiv.org/pdf/1709.04959.pdf

https://www.facebook.com/help/379220725465972

https://www.youtube.com/watch?v=N91ZdtqgZIU

https://www.youtube.com/results?search_query=the+2+step+verification+option+is+a+good+idea

Social media and the wellbeing of children and young people: A literature review:

http://www.uws.edu.au/__data/assets/pdf_file/0019/930502/Social_media_and_children_and_young_people.pdf

Children and Youths in a Digital World - UNICEF REPORT 2017:

https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf

The Educator's Guide to Social Media - www.Connectsafely.org

Helping Parents keeping their children safe online

www.Internetmatters.org

National Centre for missing and Exploited Children - www.Netsmartz.org

https://whatis.techtarget.com/definition/social-media

https://en.wikipedia.org/wiki/Cyberpsychology

https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/be-aware-of-fake-social-media-accounts-and-fake-mobile-apps

References for the methodological part:

http://www.academia.edu/25119518/Colec%C8%9Bie_de_bune_practici_pentru_tineret_100_metode_%C8%99i_situa%C8%9Bii_nonformale

https://beldie.ro/parola/

https://www.go4it.ro/internet/cum-alegi-o-parola-sigura-tot-ce-trebuie-sa-stii-despre-parole-5789165/

https://playtech.ro/2018/cum-alegi-o-parola-sigura/

https://www.emiral.ro/blog/ce-sunt-parolele-si-cum-ar-trebui-sa-arate-o-parola-sigura/

https://www.sfaturi.net/cum-iti-creezi-o-parola-puternica-sigura/

https://askit.ro/solutii/cum-sa-iti-tii-parolele-in-siguranta-cu-dashlane-manager-de-parole/

https://antivirus-free.ro/util/verifica-ti-parola-cu-ajutorul-kaspersky-secure-password-check.html

https://playtech.ro/2018/parola-perfecta-cum-securizezi-orice-cont-online/

Credits for pictures used in this document:

https://unsplash.com/photos/e3OUQGT9bWU

https://unsplash.com/photos/SpVHcbuKi6E

https://unsplash.com/photos/ourQHRTE2IM

https://unsplash.com/photos/EhTcC9sYXsw

https://unsplash.com/photos/gaXC8gn3_gM

https://pixabay.com/en/woman-face-thoughts-media-head-1446557/

https://pixabay.com/en/network-earth-block-chain-globe-3537401/

https://pixabay.com/en/network-social-abstract-3139214/

https://pixabay.com/en/icon-networks-internet-social-2515316/

https://pixabay.com/en/icon-polaroid-blogger-rss-tumblr-2486501/

https://pixabay.com/en/social-media-media-board-networking-1989152/

https://pixabay.com/en/hacking-cybercrime-cybersecurity-3112539/

https://pixabay.com/en/roulette-gambling-poker-casino-win-3832550/

https://pixabay.com/en/software-piracy-theft-cd-computer-1067128/

https://pixabay.com/en/contact-letters-email-mail-glut-2805253/

https://pixabay.com/en/email-mail-contact-letters-3597087/
https://pixabay.com/en/anarchy-punk-penguin-violence-bat-154627/
https://pixabay.com/en/credit-card-bank-card-theft-1591492/
https://pixabay.com/en/bully-attack-aggression-bullying-655660/
https://pixabay.com/en/binary-black-cyber-data-digits-2170630/
https://pixabay.com/en/play-card-game-poker-poker-chips-593207/
https://pixabay.com/en/enter-sign-password-membership-1643453/
https://pixabay.com/en/binary-one-null-man-person-503578/
https://pixabay.com/en/gdpr-data-protection-privacy-3438462/
https://pixabay.com/en/internet-computer-screen-monitor-1593384/
https://pixabay.com/en/register-sign-up-password-username-2819608/
https://pixabay.com/en/digital-road-sign-security-close-579553/
https://pixabay.com/en/social-media-you-tube-facebook-1177293/
https://pixabay.com/en/human-google-polaroid-pinterest-3175027/
https://pixabay.com/en/revelation-transformation-awareness-2937691/
https://pixabay.com/en/fingerprint-unlock-network-man-2904774/

1.8. Further reading suggestions

https://www.europol.europa.eu/newsroom/news/15-ways-you-could-be-next-victim-of-cybercrime
https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation

Chapter 2

Cyberbullying - between Game and Misdemeanor

2.1. Introduction

“Data Protection in the Virtual Environment”, the first chapter of this guide, focuses deeply on issues concerning online safety and the risks of using certain apps and social networks. Indeed, it offers a great deal of information and tips on how to be safe online, and how to protect ourselves and those we love from potential dangers. In this respect, the first chapter also mentions that younger people are exposed to cyber-aggression, a phenomenon which consists of using social media deliberately to upset, threaten and intimidate someone else.

Cyberbullying is one of the main challenges of the 21st century and, as such, it is becoming increasingly necessary to know the dynamics of any cyber-attack in order to defend ourselves against this phenomenon. The digital era we are living in needs people to become more aware of the risks of online harassment. As a result, the purpose of “Cyberbullying - between Game and Misdemeanor”, the second chapter of this guide, is to give an account of the differences between traditional bullying and cyberbullying as well as to provide a better understanding of the dynamics of such a phenomenon.

This attempt becomes even more important if we consider that cyberbullying lacks a shared definition and approach at European level, since it falls within the additional competences of the European Union. In addition, many member States do not provide a specific definition of cyberbullying in their national legislation, thus hampering even more of the possibilities for a shared understanding at European level.

Therefore, the aim of this guide is to analyse the impact of online harassment in the countries involved in the BEWARE project and contribute to the development of a common approach at European level in order to combat the episodes of cyber-aggression.

More precisely, 75 young people, aged between 15-20 years, were selected and were asked to fill in a questionnaire to analyse the degree of knowledge and the perception of this phenomenon. What the data suggests is that participants are aware of cyber-bullying being a nowadays reality since they experienced it firsthand and, as such, they are aware of the risks they take when they use social media. Nevertheless, the results show that the 55% of the participants do not actually know when cyber-aggression can be called this way, while some of the others think that cyber-aggressions are related to threats (mental or physical) and offenses. Also, concerning the cyber-bullying phenomenon, they realize that there is a difference between an harassment and a joke but they do not actually know how to define cyber-aggression.

Finally, participants confirmed that there is a growing need for spreading awareness about this phenomenon, since part of the problems nowadays seems to be related to the limited knowledge about effective prevention and intervention tools and how to implement them.

As far as the structure of the second chapter is concerned, the first part defines the phenomenon of cyberbullying and its various manifestations. The attempt of the second part of this chapter is to give advice on how to deal with cyberbullying and how to prevent it. This guide is also addressed to youth workers who want to tackle this issue with other young people. For this reason, non-formal activities related to the topics covered have been included in a specific toolkit for youth workers.

2.2. Cyberbullying at European level

The definition of a common approach about cyberbullying at European level is still far from being achieved. The main reason can be found in the limited role assigned to European Institutions concerned the field of cyberbullying prevention, where the EU has only a 'supplementary' role consisting mainly of supporting, coordinating or supplementing the initiatives adopted by the Member States at domestic level[1].

Nevertheless, among the major initiatives that have been taken at European level in this regard, it is worth mentioning the following ones:

- Multiannual Community programme on protecting children using the Internet and other communication technologies.

[1] "While both the Lisbon Treaty and the Charter provide legal grounds for EU action in the area of children's rights, neither of them confer a competence on the EU as a general policy area. Under the principle of conferral set forth in Article 5(2) of the TEU237, the EU can only act within the limits of the powers assigned to it. The EU may have 'exclusive', 'shared' or 'supplementary' competence. Competencies not conferred upon the Union in the Treaties remain with Member States. This is the case for cyberbullying, for which the EU has only a 'supplementary' role consisting of supporting, coordinating or supplementing the initiatives adopted by Member States at domestic level." http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf

- Daphne III Funding Programme.
- Safer Internet Day.
- European Anti-Bullying Network.

Similarly, different legal aspects indirectly concerned with this phenomenon have been covered and can be applied to cases of cyberbullying and online harassment: expressions of racism and xenophobia, support and protection of victims of crime, sexual harassment of a victim under 18, procedural safeguards for children accused in criminal proceedings, data protection regulation.

At domestic level, the majority of practices adopted by the Member States against cyberbullying are already part of existing provisions in their penal codes, but only half of them have specific laws in regards. Similarly, until 2016 only 14 members states had developed an official definition of cyberbullying, which, in the majority of cases, was limited to defining it as a form of bullying taking place online.[2]

2 http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf#page=167

2.3. Bullying and Cyberbullying: *what, where, who and why*

Bullying is a phenomenon that is becoming more and more common among teenagers, but as results of the Beware questionnaire show, children don't really know how to recognize and define it. For this reason, before starting analyzing the phenomenon of bullying, we need to give a simple and general definition of what it's meant by "bullying":

"Bullying is an unwanted, aggressive behavior among school-aged children that involves a real or perceived power imbalance. The behavior is repeated, or has the potential to be repeated, over time." – Stopbullying.gov

According to this definition, we can talk about "bullying" when an aggressive behavior presents also the following characteristics:

- **Intention** to harm → the bully *wants* to hurt the victim

- **Repetition** over time → the aggressive behavior takes place *multiple times*
- **Power imbalance** between the victim and the aggressor → the bully wants to hurt the victim multiple times and make him/her *feel vulnerable*

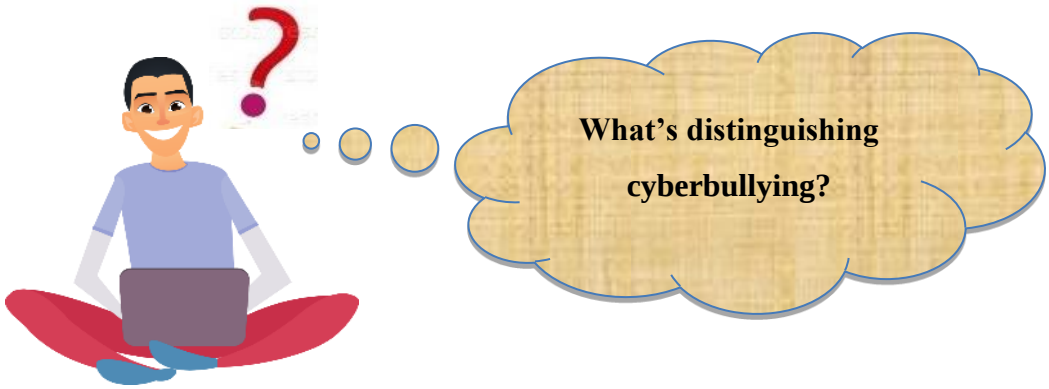
We've now defined what bullying is and its main characteristics, but unfortunately we cannot resume all kinds of bullying under one single word. Bullying has many faces and, in order to understand when a bullying episode is happening, it's important to firstly learn how to distinguish one from another. In fact, bullying can occur in multiple ways:

- **Verbal bullying:** Name calling, starting rumors, negative teasing, threats.
- **Social or relational bullying:** Excluding others from the group, ignoring and shunning, gossiping, spreading rumors, telling secrets.
- **Physical bullying:** Hitting, kicking, inappropriate touching, sexual gestures, groping, threatening.
- **Cyberbullying:** Using e-mail, social network sites, cell phones, webcams, text messages, and Internet sites to send mean messages, spread rumors, post embarrassing pictures or videos and fake websites or profiles.

In this guide we will concentrate on the last type of bullying, the one that usually occurs online and that, due to the increasing use of social media, is becoming more and more common: cyberbullying.

By defining cyberbullying as a sub-category of bullying, we can guess that both cyberbullying and "normal" bullying, represent a dangerous and equally serious issue. Nevertheless, the former owns some particular characteristics that make it even more endangering and more difficult to cope with.

As the table shows, cyberbullying owns three characteristics that help us to distinguish it from any other type of bullying.



NORMAL BULLYING

- Intention to harm
- Repetition over time
- Power imbalance between the victim and the aggressor

CYBERBULLYING

- Intention to harm
- Repetition over time
- Power imbalance between the victim and the aggressor
- Use of electronic or digital means
- Sense of anonymity and lack of accountability
- Publicity

First and foremost, cyberbullying is based on the use of electronic and digital means, such as computers, smartphones and tablets, which gives the bully a wide range of devices to choose among to bother the victim. Secondly, cyberbullying happens in cyberspace, a place with multiple venues where billions of people can easily hide. The screen suggests a sense of anonymity that pushes people to be bolder and to say things we would never say face-to-face. Cyberbullying usually happens in the comfort of your own house and can transform it into a

very uncomfortable place due to the mental violence that aggressors are perpetrating. The fact that it doesn't involve a physical aggression, in this sense, doesn't make it less dangerous.

Finally, cyberspace, and in particular social media, is a public arena where everything is public and everyone is allowed to share his thoughts about someone else, even if those thoughts are bad and insulting. The visibility of such comments online as well as the difficulty in removing inappropriate information posted by someone else, makes cyberbullying even more violent and alarming.

2.3.1. The blurring line between cyberbullying and jokes

The definition of cyberbullying helps us to distinguish a bullying episode from a simple joke. It's very important to learn how to do that, because in order to cope with the problem and seek for help we should be able to recognize it in the first place. In fact, one of the most alarming results of the research led by the BEWARE project is that, even though teenagers are aware of the difference between cyberbullying and jokes, the 55% of the interviewed admits that they are not able to give a concrete definition of “cyber aggression” and wouldn’t know how exactly cyber aggression can be identified as such. As a consequence, the possibilities to confuse a cyberbullying episode with an innocent joke are potentially high.

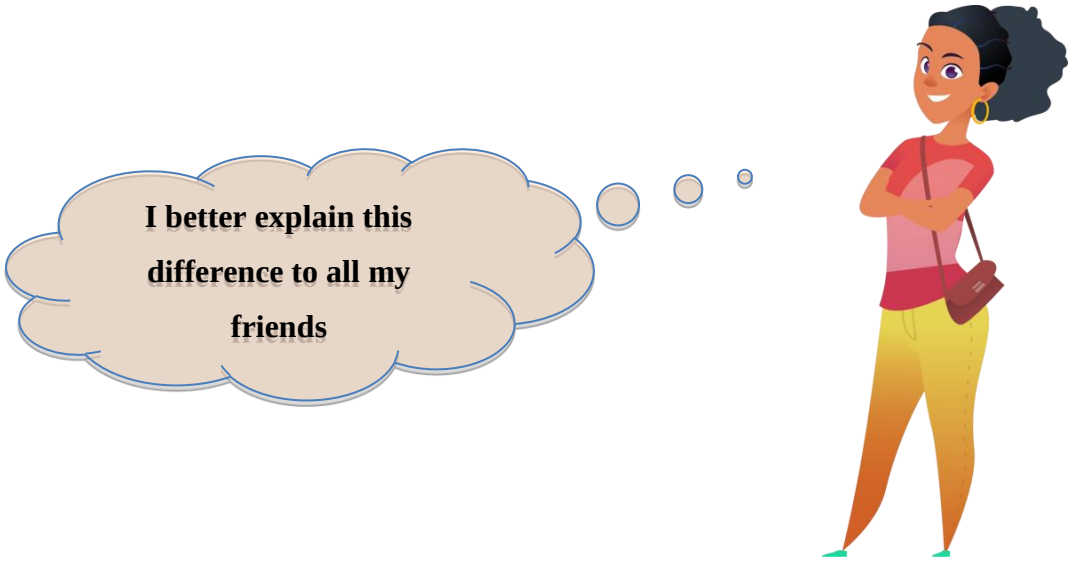
The same can be said for the other categories of bullying which, as in the case of cyberbullying, do not involve a physical aggression. Teasing is a common aspect of young people’s interaction and, when done in the right way, can actually be a very positive way of communication and creation of bonds. Children can use it to create new relationships or try to change someone's behavior, but in both cases it's a harmless way to exchange jokes back and forth. One of the main distinctions between a joke and bullying is that, in the former case, if the teased child gets offended the tease eventually stops because the comment wasn't meant to be hurtful in the first place. Nevertheless, there are also other distinctions which help us to pay attention to our way of interacting with other people.

Positive teasing

- It takes place within a strong relationship with two people who appreciate the teasing as affectionate
- The teaser is using a "joking" (rather than aggressive) tone of voice and smiling
- The person being teased does not look distressed

Bullying

- The content of the teasing turns from affectionate to hostile
- There is a power imbalance: the person teasing has more power among peers compared to the person being teased
- The teasing occurs repeatedly
- The child who is teasing means to upset or hurt the child being teased
- The child being teased is upset or hurt by the interaction

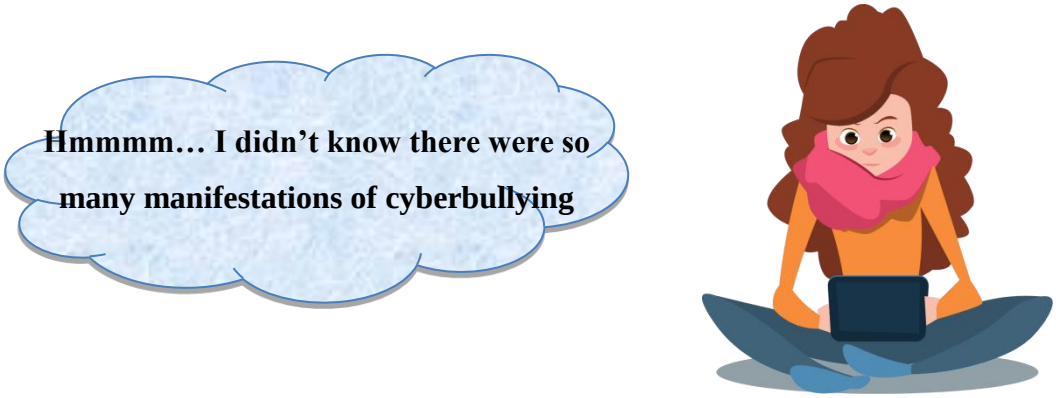


2.4. The multiple manifestations of cyberbullying

Once we've defined the phenomenon and learnt how to recognize it, it's time to think about *where* episodes of cyberbullying can take place. In fact, unlike "normal" bullying, cyberbullying doesn't happen in the park right in front of our house or at school; cyberbullying happens in the cyberspace, an undefined place where billions of anonymous people can interact among themselves in different ways. In this sense, it's important to investigate where cyberbullying can take place. Participants affirm that cyberbullying episodes are likely to happen on any kind of social media, even though probabilities increase even more when it comes to those with a private-messaging function.

- **Texting –** It doesn't always have to be someone you don't know. Sometimes the aggressor is someone you know very well, someone who has your cell phone number and knows how to hurt you. Teenagers tend to hide their messages and make sure that nobody except them has access to them. That's why it's becoming more and more difficult to fight cyberbullying: most of the time we don't even realize something is going on and youths, especially during the teenage years, can be very hurtful.
- **Instant messaging –** Instant messaging is just another variety of texting. The worse side? Even people you don't know can send you a message. Nowadays, almost every website has an instant messaging platform where users can meet each other and start chatting. For example, loads of video gaming websites have their own instant messaging platform that could easily be transformed into a means to start offending other players, especially if the game is not going the way we planned.

- **Social networks –** Social networks are like a window that directly shows our life, even if we didn't mean to. Pictures can be posted without our consent, we can be tagged on posts, we can share our thoughts, ect... It's the easiest way to let someone into our lives, but it can be as beautiful as dangerous: bad comments can be left under our posts, screenshots of our pictures can be taken and shared without our consent, and once we have shared our data with the net, it's very difficult to permanently remove it.
- **Anonymous apps –** These apps allow to create posts anonymously (which doesn't mean that data is not being registered), chat with new people, share pictures and videos. The fact that you don't have to share your identity often leads to racial abuses or violence threats.



2.5. The Aggressor

Today's society makes it very easy to become a bully. We are surrounded by electronic devices, everybody has access to social media and people are spending more and more time online than ever before. But *who* are these people? *Who* is the aggressor? Do we know him?

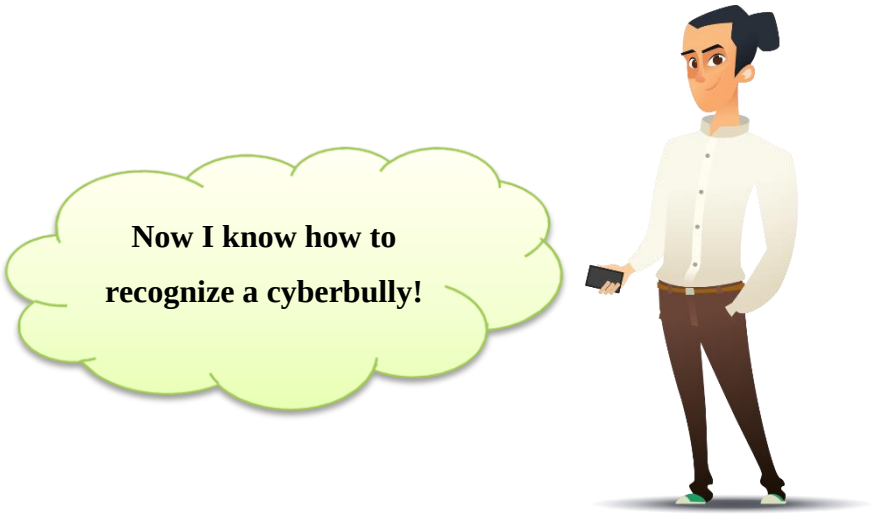
We can define the cyberbully as it follows:
"a group or an individual that carries out an aggressive, intentional act or behaviour through images, negative comments, insults and threats on social media sites, repeatedly and over time against a victim who cannot easily defend him or herself". (Smith, Mahdavi, Carvalho, & Tippett, 2006, p.1)

Sometimes, yes, as we said earlier, the aggressor can be someone we do know, and that maybe we actually know pretty well, someone we see everyday at school. But as we are talking about cyberbullying, most of the time the aggressor is someone we don't know and that we've never seen in our "real" life, and that makes things even more difficult because we can't tell who is hiding on the other side of the screen.

Nevertheless, regardless of whether we know them or not, cyberbullies have some general characteristics in common:

- They enjoy controlling others and perform a dominant personality;

- They do not show empathy and compassion for the victims. This is due to the fact that they generally do not realize the consequences of what they are doing;
- They feel more powerful than the others. As we said, in fact, all types of bullying concern a perceived imbalance of power between the victims and the aggressors;
- They enjoy conflicts and they look for them;
- They refuse to accept responsibility for negative behaviors.

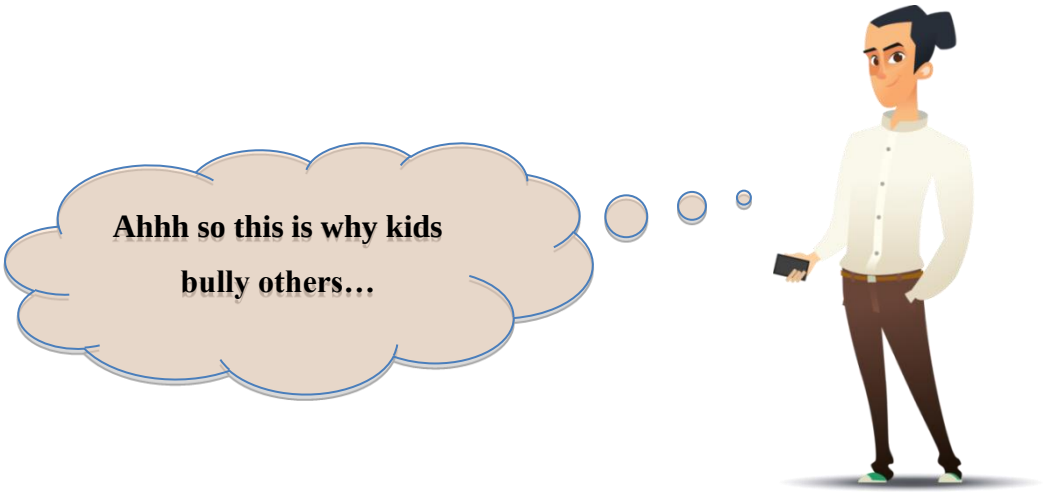


2.5.1. Why do children bully others?

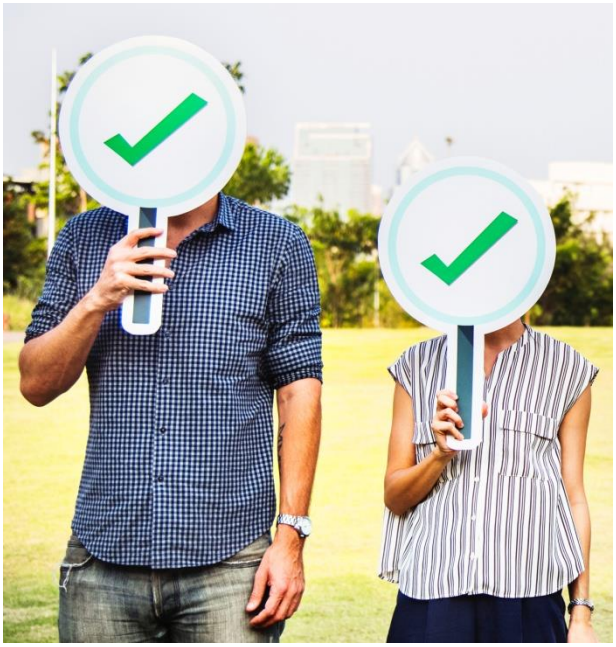
We have now defined *what* cyberbullying is, *where* it happens and *who* is the aggressor. But the real question that should come to our mind when we think about cyberbullying is: *why* do kids bully others?

- **Power –** Teens who like to be in control and have power are more inclined to become bullies. When things don't go the way they planned, they start performing bullying behaviors in order to establish their supremacy again. This usually happens when a kid wants to have power over smaller or weaker students, or when competition is involved and someone wants to affirm himself over the other competitors.
- **Peer Pressure –** The teenage world can be a very hard and cruel place where to live. Everybody wants to fit in, and the need of being accepted and the fear of being the next targeted kid are good enough reasons to start bullying others.
- **Prejudices –** A different race, religion, sexual orientation. A different diet, a special need. Being different is always a hard thing to cope with, especially during teenage years, when prejudices always lead to a new root to start bullying.

- **Payback –** Sometimes, kids who have been bullied in the past become bullies themselves. Usually these kids feel justified for their actions and feel a sense of relief and revenge for what they have experienced.
- **Popularity –** Social status is important when you are a kid and are trying to affirm yourself. Popular kids make fun of less popular kids, spread rumors and ostracize others. They also do that to get attention or to diminish the social status of another kid that they feel might become more popular than they are.
- **Personal problems –** Kids who have a difficult home-background are more likely to become bullies to regain the control they feel is lacking at home. Teens who have low self-esteem due to abuses may resort to bullying to cover the lack of self-worth.
- **Pleasure –** Sometimes kids are bored, and in order to add some excitement to their lives they may start bullying others. They may also experience a lack of attention from their parents, and bullying may help them get some of the attention they're missing. Also, sometimes kids lack empathy and actually enjoy hurting other people's feelings. They also appreciate the sense of power they get from bullying and find their hurtful jokes funny.



2.5.2. Gender of the cyber aggressor



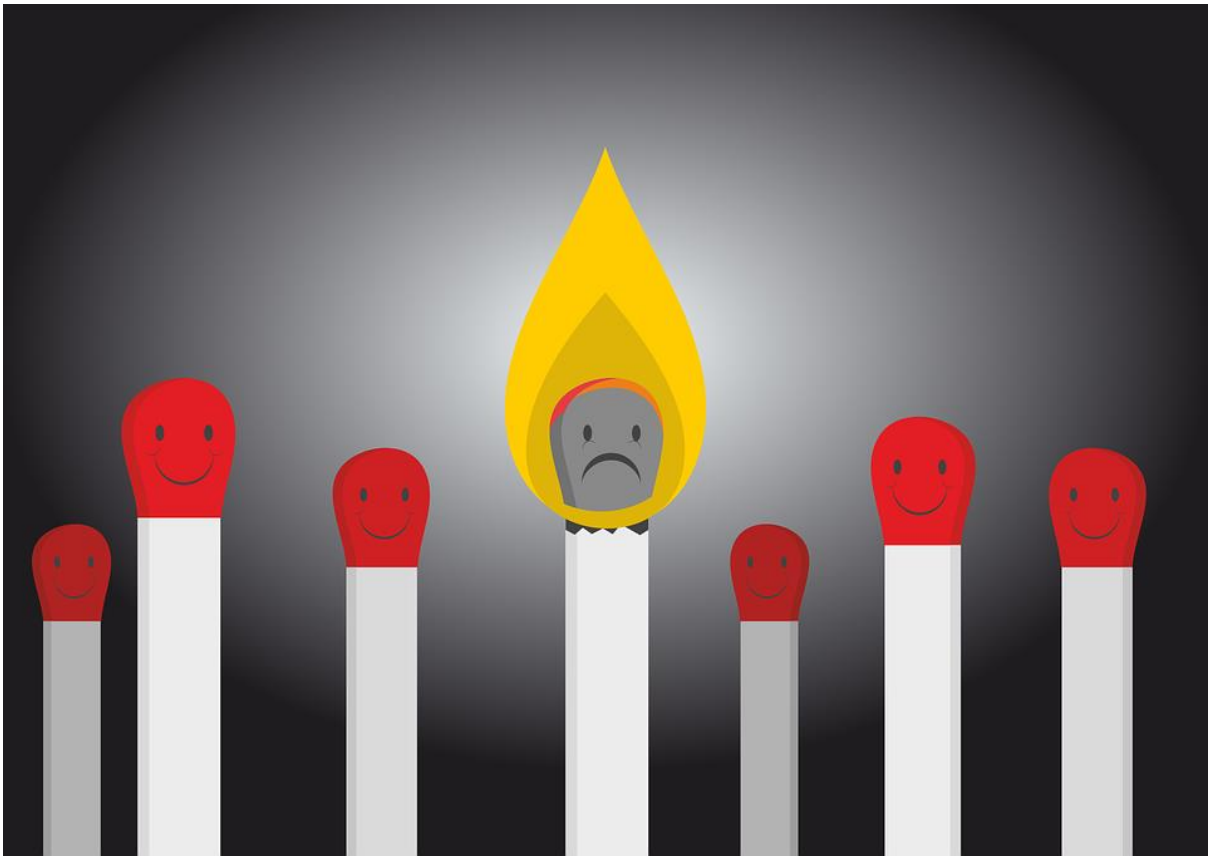
When comparing the findings with those on traditional bullying, where boys tend to bully more than girls, evidence suggests that cyberbullying is generally equal for both sexes. Although some studies suggest that girls are perpetrators of cyberbullying as much as boys, no conclusive evidence can be drawn on this aspect.

The fact that girls are more involved in bullying online than offline may result from the indirect nature of electronic communication and the opportunities it presents for group social interaction. Research shows that while boys tend to be more aggressive and are often involved in physical bullying, girls tend to use emotional tactics.[3]

Girls tend to be more covert in their bullying tactics (e.g. sending intimidating emails from a fake account or spreading rumours about their victims). The means used to perpetrate cyberbullying seem to be linked to gender differences. Girls seem particularly active in social media. As a result, it was found that more girls bully on social networks than boys.

[3] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3881143/

2.6. The bystander



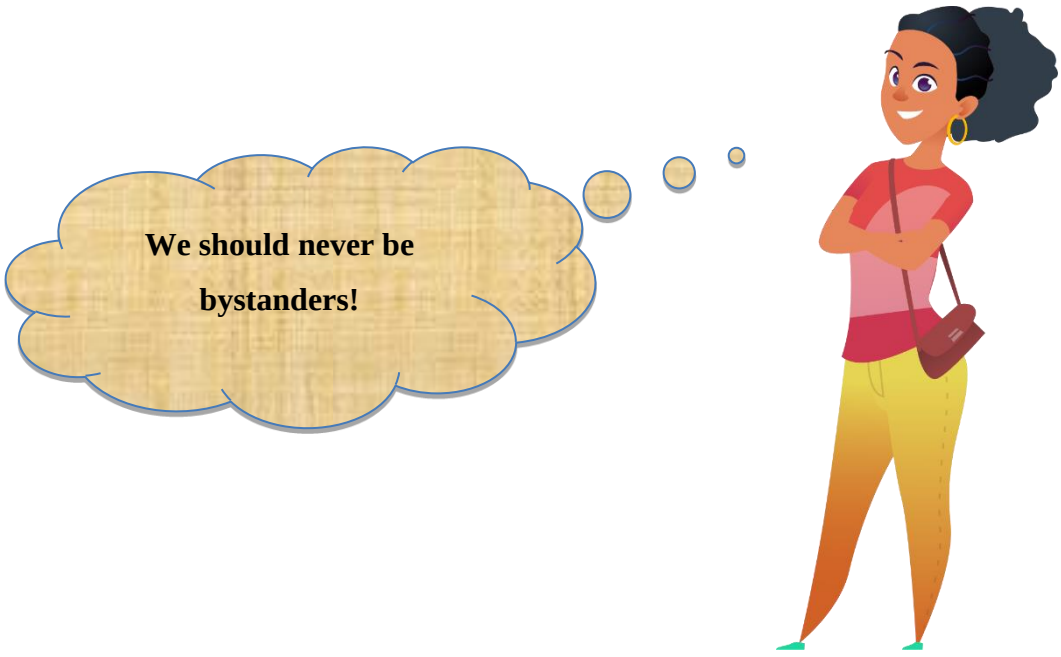
The bystander is someone who sees what is happening between the bully and the victim but is not directly involved in the bullying episode. In traditional cases of bullying, the bystander's role is limited to that of witness. Digitally, the numbers of bystanders can be thousands or in some rare cases millions as a result of content spreading virally online.

Also, as reported in the Beware questionnaire, the vast majority of the participants is aware of cyberbullying episodes such as shaming, insulting, posting pictures without consent and stealing identities and personal data.

When it comes to cyberbullying, there is no clear distinction between a perpetrator and a bystander. While bystanders in traditional bullying are just passive or encourage the perpetrator,

bystanders in cyberbullying can actually be involved in the incident. If a perpetrator posts derogatory content about a victim online and bystanders choose to share the content their role becomes similar to that of the cyberbully. In this respect, the results of the Beware questionnaire shows the 80% of the participants agree on the fact that those who witness a cyber-aggression and do not report it are responsible too, while the 19% gave "Maybe" as an answer and only 1% of them thinks that witnesses are not responsible.

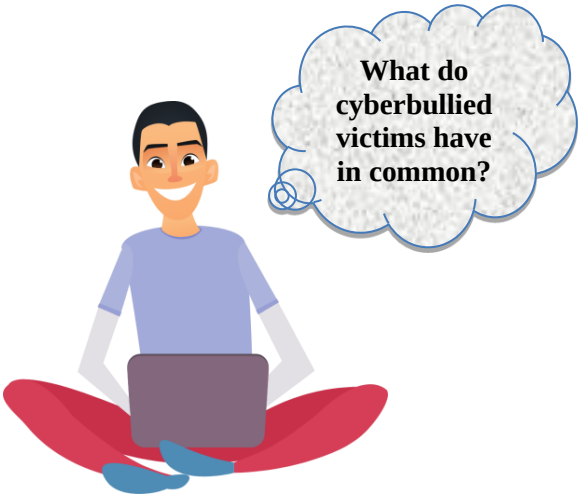
By consuming, liking and sharing the harmful content, bystanders may, thus, reinforce the behaviour of perpetrators. [4]A recent study has found that compared to face-to-face situations, bystanders are even less likely to intervene with online bullying. For instance, it has found that bystanders are reluctant to take action when the victim is someone they do not know well, however this amount decreases when the victim is a close friend of the bystander.



[4] https://www.universityofcalifornia.edu/news/who-speaks-against-online-bullying

2.7. The cyber victim

Every victim of cyberbullying displays certain characteristics, but in the most of the cases students are likely to be bullied because of a number of perceived vulnerabilities, such as the student's appearance or body size, the degree of masculinity or femininity, the performance in school, the perception of being gay, lesbian, bisexual or transgender, as well as the student's low income household, his/her race, ethnicity, national origin or religion, and disabilities or any special health needs.



Similarly, there are also some unperceived vulnerabilities which increase the likelihood to become a victim of bullying. In other words, cyberbullied have some general characteristics in common:

- they are shy and with low self-esteem;
- they are insecure, anxious and sensitive, with problems with the correct encoding and interpretation of emotions;
- they have less developed emotional connection with their parents;
- they have less connection with school;
- they spend more time online;
- they use more aggressive or passive coping strategies;
- they have negative self-related attitudes.

For this reason, we can define the victim as an individual who presents particular difficulties, physical or psychological disabilities, problems in establishing social relationships or belong to a minority group. Victims of cyberbullying may not know the identity of their bully, or why the bully is targeting them.

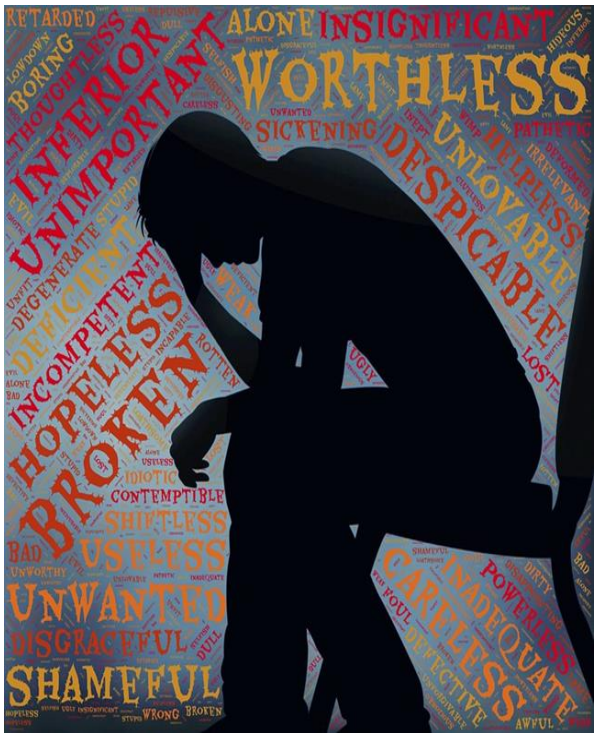
2.7.1. Gender of the cyber victim and influential factors

Research has indicated that girls are more likely to be bullied online. The high presence of girls among victims may be due to the fact that girls are more likely to report cyberbullying episodes turning more than boys to their parents and friends for help. As the results of the Beware questionnaire suggest, almost every participant, especially if female, would report a cyber-aggression if it occurred to her/him, and they indicated the police, their parents and the network administration as the most common authorities to whom to report the episode. Unlike girls, boys might tend to underreport incidents due to societal constructs on male identity. This behavioural factor should indeed be taken into consideration as it may be that boys do not always report when they have been bullied.

The type of school attended also has a strong influence on the likelihood of being a victim of cyberbullying. To give an example, at the high school, a small percentage of the pupils are victims whereas at a non-selective secondary school a greater percentage of the pupils are affected by bullying online.

Furthermore, the type of internet use has a strong influence: ‘cyber-fixed’ profiles (high internet consumption) are more affected by cyberbullying whereas ‘cyber-distanced’ profiles (lowest internet consumption) are less affected.

2.8. The consequences of cyberbullying



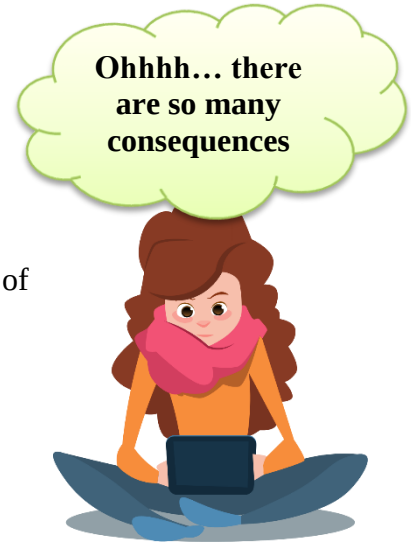
Bullying can affect everyone — those who are bullied, those who bully, and those who witness bullying. Here are some common feelings that protagonists of cyberbullying often experience:

In the aggressor:

- Increase in problem behaviours including higher levels of proactive and reactive aggression, property damage, illegal acts, substance use, smoking, drunkenness, delinquency, and suicidal behaviour[5];
- Social difficulties such as stress, depression and anxiety;
- Negative emotions such as anger, sadness, frustration, fear and embarrassment;
- Increased use of punitive discipline and weaker emotional bonds with caregivers.

In the bystander:

- Reinforcement of individualistic and selfish behaviour;
- Lack of empathy with the pain of the victim;
- In some cases, feeling of helplessness similar to that of the victim.



[5] Retrived from: https://www.stopbullying.gov/at-risk/effects/index.html

In the victim:

- Problems of low self-esteem and lack of self-confidence;
- High levels of loneliness and anxiety, suicidal ideation;
- Difficulties in school integration and in the learning process;
- Social mismatch and isolation;
- Anger and frustration;
- Clinical symptoms such as neurosis, hysteria and depression;
- Physical health concerns such as problems sleeping, poor appetite, skin problems, headache;
- Unleashed violent attitudes;
- Fewer relationship and more emotional and peer relationship problems.

The results of the Beware questionnaire in this regard are unambiguous: the most common consequences of cyberbullying on the victim that have been identified by the participants are depression, anxiety, self-harm, low self-esteem, eating disorders and suicide, and participants suggest psychological help in order to give support to the victims.

Statistics from the National Crime Prevention Council's 2010 Cyberbullying Prevention Research study

EMOTIONAL

- Becomes withdrawn or shy
- Shows signs of depression
- Is extremely moody or agitated
- Is anxious or overly stressed out
- Shows signs of aggressive behavior

SOCIAL/BEHAVIORAL

- Suddenly stops using the computer
- Changes eating or sleeping habits (e.g., nightmares)
- No longer wants to participate in activities once enjoyed
- Hurts self, attempts or threatens suicide
- Suddenly changes friends

The biggest red flag is a withdrawal from technology. If you notice a sudden change in computer or phone usage, talk to the child. They may be being cyberbullied.

For more information check out www.ncpc.org

ACADEMIC

- Doesn't want to go to school
- Gets into trouble at school
- Skips school
- Loses interest in school
- Drops in grades

SIGNS THAT A TEEN MAY BE CYBERBULLYING OTHERS

- Stops using the computer or turns off the screen when someone comes near
- Appears nervous or jumpy when using the computer or cell phone
- Is secretive about what they are doing on the computer
- Spends excessive amounts of time on the computer
- Becomes upset or angry when computer or cell phone privileges are limited or taken away

2.9. Are you a victim of cyberbullying? Here's how to cope with the problem

First and foremost, it's quite obvious that you should avoid giving personal pictures, telephone numbers, addresses or any other kind of personal data. Better safe than sorry!

But if it's too late, here's some advice:

- Try not to reply with anger. Keep calm, or you'll just make it easier for the cyberbully to hurt you.
- Be firm with your answers: you'll look stronger and tougher and the aggressor could be discouraged. On social media there is no physical contact, which is helpful in this case because nobody will see your real reaction. Fake it through 'til you make it come true, keep calm!
- Ask a friend to help you answer the cyberbully

- If the cyberbully keeps harassing you, you try to ask him to stop! There is no guarantee of success, but is an attempt you should try in order to show that you are not going to accept abuses anymore.
- Seek for help! Talk to the people you know will listen to you and that will try to help you out: a teacher, your parents...
- Block the cyberbully! Probably he won't stop anyway, but at least you will be less tempted to reply.
- Don't be afraid to talk to an adult. You won't be punished: trying to ignore the problem or minimize it won't be helpful. it could get things worse instead.
- If the harassment is going on on your email, change your address. One useful method to avoid harassment is to ignore the bully.
- Contact the social network management system and ask to remove any of your personal data. The material won't be deleted, but people won't have access to it.
- Save proofs. The cyberbully disadvantage is that you can save every insult and threat. Use them wisely!
- If the cyberbully doesn't remove the content within 48 hours you can make a complaint to the European Data Protection Supervisor, even if the identification of the person that posted the non-authorized content is not possible. The intervention of the Data Protection Supervisor will take place within 48 hours.
- If you are threatened of physical damages, don't hesitate to call the police! Ask a parent or any other adult to call the law enforcement.
- Take into consideration the possibility to talk to the school authority.
- Protect your accounts and your mobile phone! Don't share your passwords with anybody: it could be very dangerous to share it.n

REMEMBER: seeking for help in order to stop these bullying episodes IS NOT a symptom of weakness. It just means that you are not willing anymore to accept threats or bas teasing! Furthermore, seeking for help could push other kids in your situation to do the same. Many bullying episodes could fall into the category of misdemeanor: that's why it's important to talk to people such as trustworthy adults. Confronting more experienced people could help you understand the seriousness of the situation and how you should behave after a cyber-aggression episode.

2.10. Do you know somebody who is a victim of cyberbullying?

If you know somebody who is a victim of cyberbullying, *don't be a bystander*: ACT! A **bystander** is someone who witnesses an episode of cyber-violence without intervening. The best thing to do to stop these episodes is to stand against them.

- **Report the episode to the school authority.** If the victim is one of your schoolmates, report it! You can report the episode anonymously without exposing yourself to any risk.
- **Report the episode to the website/app/game.** Every respectful social network or platform forbids cyberbullying and gives easy tools to report violations while keeping your identity safe.
- **Talk to a trustworthy adult.** Tell an adult that you can rely on what happened if a classmate had a bad experience online. A parent, a teacher, your trainer or any other adult would be okay, what's important is that the person you are talking to is **trustworthy**.
- **Collect evidence.** Take a screenshot, save the picture or the message, record with you phone the episode. This way the adult you're talking to will be able to intervene with proofs in his hands and will be able to observe the abuses the victim suffered.
- **Show true interest.** Show your classmate that he is not alone. Send some encouragement messages or pictures. Tell him you care and show him how much you're interested in his situation: he won't have to cope with the situation all alone, but he will be able to count on you. Also, why don't you try to involve other classmates too? You

could post some positive comments under one of his pictures or one of his posts. Remember: there is strength in numbers!

- **If you know the cyberbully, tell him to stop!** Try to make him understand that is not cool to behave like a jerk with other people. It's important not to stay quiet: if you don't say anything you could encourage the bully to keep behaving like that.
- **Do not encourage the bully.** If you witness cyberbullying episodes, *do not encourage them in any way*. Don't add any comment that could make the bully thing what he's doing is right: avoid like, smiles or any other form of support.
- **Keep yourself safe.** Don't threaten physically other people. Avoid getting in trouble to help your friend, you could get the situation even worse! Furthermore, if you notice cruel or insulting behaviour on social media, don't be part of them, just report them!
- **Use imagination.** Think in a creative way about what could stop a cyberbullying episode. Share your opinion with others and use everybody's talent to find a solution.

2.11. Cyberbullying and the importance of prevention

In an era in which we are becoming increasingly dependent on the internet and social networks, we are witnessing an increasing number of cyberbullying acts or cyber attacks in general. Such situations can be extremely unpleasant and awful for the victims.

When we speak about cyberbullying there are several factors that we have to consider, *in the first place* the importance of **prevention**. It is actually possible to fight cyberbullying episodes simply by prevention, but to ensure that this will happen, the online users must have a certain degree of **knowledge** about the instrument they are using. Therefore, it becomes important the family role in educating their children to use properly and conscientiously internet and social media.

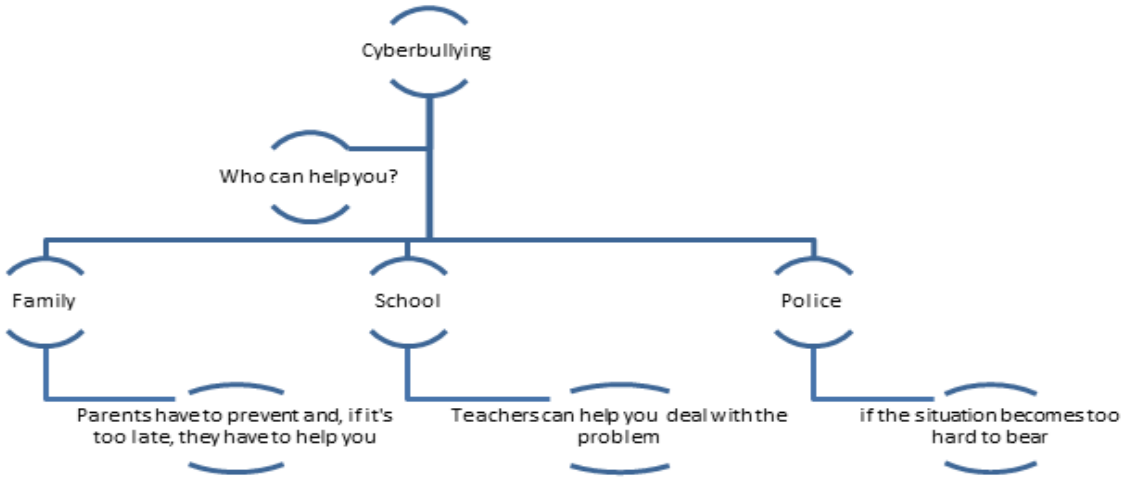
2.11.1. Tips for preventing cyberbullying

- **Inform yourself.** In order to prevent cyberbullying you have to understand exactly what it is. In what it consists? How and Where? Talk about it with your friends in order to understand their point of view and if they ever had that kind of experience.
- **Protect your Password.** Keep it a secret, don't even say it to your best friend! But if someone comes to know it, you are always in time to change it.
- **Think.** Before posting any of your photos on a social network, send it to friends or other people you trust. Those who want to hurt you can use it as they like to ruin your life.
- **Never open unknown messages.**
- **Always log out from online platforms.**
- **Increase your awareness.** Create a movement or a group, or an awareness-raising campaign. If we all come together we can prevent this phenomenon, especially if we would be more conscious.
- **Configure your privacy settings.** On the majority of social networks you often have the option to change who can see what you post. Accordingly, before accepting any new friendship request think it through!

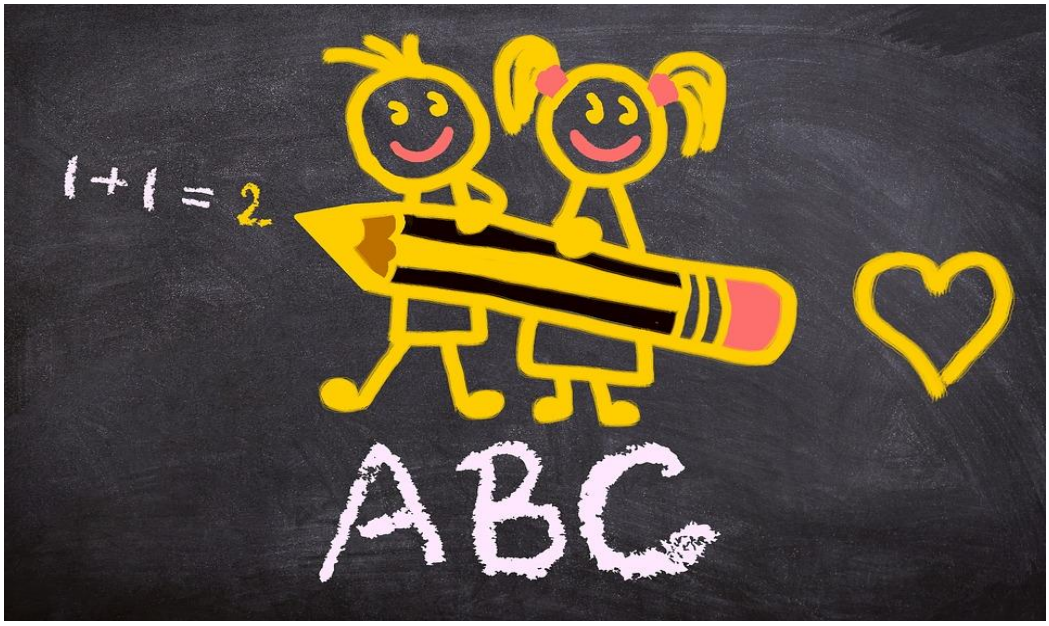
- **Search your own name over search engines like Google (egosurfing).** If you could find your name after such research, try to remove the available information before it's too late!

….And obviously don't be a cyberbully yourself !

The juvenile victims of these kind of episodes can, in case it is too late, rely on these 3 institutions: **the family** (social instruction), **the school** and **the police**.



2.12. The importance of school in preventing and protecting victims

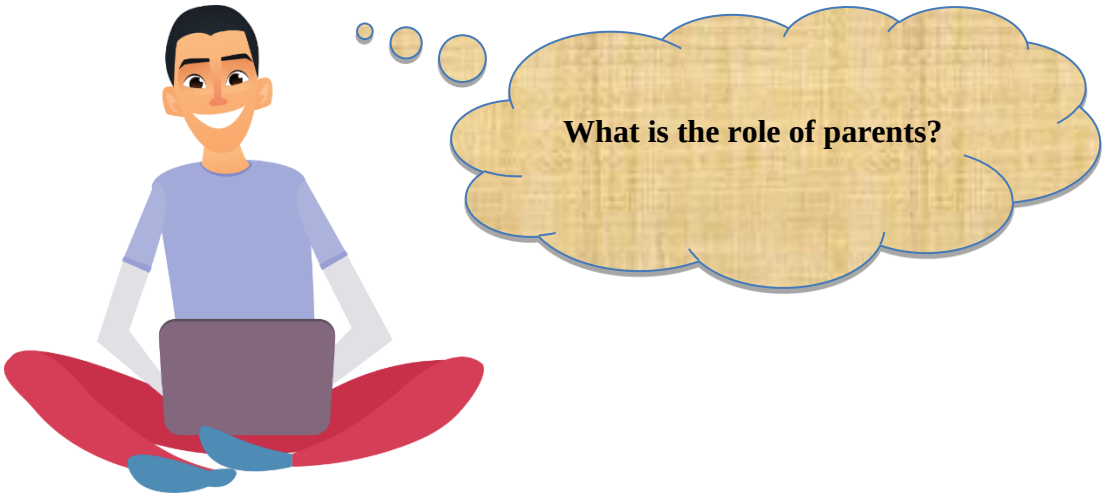


The role of the school in educating young people about mutual respect and in proper use of the internet, especially social media, is extremely important. Whenever the school Director comes to know about cyberbullying acts against a pupil of his school, he will have to inform promptly the parents of the involved children. The school rules must provide disciplinary measures in accordance with the seriousness of the acts done. It is also appropriate to save on the computer the information which can serve as proof and then, if it possible, delete - or get the platform operator to remove - all the content posted online.

When it comes the schoolmates to be involved, it is advisable that the parents contact the teachers themselves and, if there's one, to the school psychologist to consider reporting the incident to the police. So it is up to the school providing education and information, do prevention and takes act on problems afflicting children, to enhance their well-being and ease their discomfort.

2.13. How your parents can help you in case of an cyber-attack

Keep a relationship of trust with your parents, tell them in what way you use social media. In the first palace come to an agreement in which way the might assist you on your use of digital media and on the posted content. In the event that you want to start acting with major freedom find an agreement with your parents; but REMEMBER, make sure that they're able to provide help in case you will need it!



2.13.1. The role of parents

When it comes to preventing and responding to cyberbullying, parental involvement in monitoring their children's online interactions and relationships is essential. Parents have to keep an eye on the screen or what the child is doing all of the time. In most of the cases, parents did not grow up in the digital age; they are not familiar with the virtual environment. As a result, it is their duty to learn how various social networking websites (e.g. Facebook, Instagram) work.

Parents are expected to talk regularly and specifically with their children about online issues. Also, they have to set time limits and discuss rules for online safety and Internet use.

Clearly, it may be difficult for parents to know whether a child has experienced cyberbullying. If the common cyberbullying indicators are present, parents can be encouraged to communicate their concerns to the child and offer their support. They must be supportive and understanding if their children are being bullied, and try to find out how long the bullying has been going on.

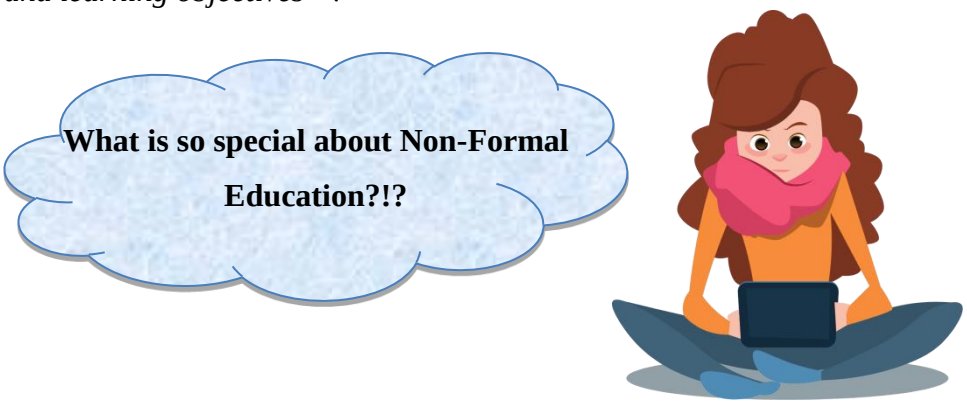
The first step to prevent cyberbullying before it becomes worse is telling their children not to respond to any cyberbullying threats or comments online. In addition, it is important not to delete any of the messages as well as everything related to the cyberbully (e-mail addresses, online screen names, etc.).

Then, parents should report the incident/s to the school as soon as possible, and ask for its help. Indeed, communication and relationships between parents and school personnel are critically important in recognition of cyberbullying attack. In conclusion, parents need to protect their child and be the ones their kids go to when something is wrong.

2.14. Non-Formal Education to tackle cyberbullying

There are many different ways to tackle cyberbullying and spread awareness among young people, but what the BEWARE Project suggests that the most effective one could be Non-Formal Education (NFE). But what is it?

The definition of Non-Formal Education provided by UNESCO-UNEVOC is "*any organised educational activity outside the established formal system that is intended to serve identifiable learning clienteles and learning objectives*[6]*".*



NFE has special characteristics that make it different from any other kind of educational method and which make it funnier and more enjoyable for students to learn through it:

- Participation in all activities is **voluntary**
- The main focus is set on **people as learners**
- Activities and methods are always designed for a particular **target group**
- The learning is **planned, structured and evaluated**
- It's **intentional** and **monitored**
- Experiencing, often called as '**learning by doing**', is the main working method

In order to better understand what **Non-Formal Education** is, it's important to operate a distinction between Non-Formal Education and **Informal Education**.

[6] https://unevoc.unesco.org/go.php?q=education&context=

Informal education is the truly lifelong process whereby every individual acquires attitudes, values, skills and knowledge from daily experience and the educative influences and resources in his or her environment - from family and neighbours, from work and play, from the marketplace, the library and the mass media. Every person experiences informal education in his or her everyday life, from birth to death. We learn something new everyday just by installing relationships with other people and living our lives, whereas NFE, as we mentioned earlier, is planned, intentional and evaluated by an educator.

Also, in NFE, *educator means facilitator*. Educator is the wide definition for the process of educating from all aspects while facilitator is just the person who has a specific strategy or method guiding pupils through it. Educators enable learning and facilitators encourage communication amongst the group.

But *why* should we choose NFE as the main education methodology to tackle cyberbullying and spread awareness? Actually, there are many advantages that could help us to pursue our aim:

- NFE can actively support change and have a real impact on the society
- NFE is essential to deliver and develop those concepts that cannot be simply «taught»
- NFE is useful to teach important values such as freedom, peace, respect, diversity, human rights
- Non formal methods have been successful in: social inclusion, capacity building, active citizenship, sustainable development, conflict resolution

2.15. Role games

The best way to implement this method in an educational environment is through *role game*. Why role game? Because it creates strong empathy among the participants and stimulates creativity. In fact, it's very important to encourage personal contribution in order to help kids to reflect about *their own* experience and being objective about themselves by increasing self-awareness.

Moreover, it is worth mentioning that role game is very versatile. This characteristic allows the possibility to adapt the game to our *specific target group* by playing different roles in different situations.

Role game can be very helpful when it comes to understand:

- the implications of a particular behaviour
- a social phenomenon
- particular roles and figures
- the contribution kids can give in that particular position

Also, it’s very easy to start a role game because you won’t need too much material. It will be sufficient to have:

- a background story
- objectives
- roles and rules
- practical activities

See below our **toolkit** to start implementing role game with your target group!

ACTIVITY FOR GROUPS

The thinking hats

Overview:
The group is divided into 3 groups of 5 people each. A conflict situation is displayed.

The activity involves 5 imaginary hats, each of a different color. These colors signify roles that must be adopted when an individual dons them. For example, while wearing the yellow hat, the individual must look only at the positive aspects of the situation under discussion. Conversely, the black hat signifies critical thinking and looking at negative points alone.

Discussion in groups about the conflict (each person in his own role without revealing it to the others); exploring different sides of the situation.

Presenting by the color of the hat – explaining the role that you had under the hat, how was it useful or not useful in the discussions.

Goal: To communicate the differences and to seek collaborative solutions

Yellow hat

The Yellow Hat symbolizes brightness and optimism. Under this hat you explore the positives and probe for value and benefit.

Key Words: best-scenario; benefits; positive thinking; optimism; value and benefits;

Black hat

The Black Hat is judgment - the devil's advocate or why something may not work. Spot the difficulties and dangers; where things might go wrong. Probably the most powerful and useful of the Hats but a problem if overused.

Key Words: risks; potential problems; obstacles; downsides; weaknesses

Red hat

The Red Hat signifies feelings, hunches and intuition. When using this hat you can express emotions and feelings and share fears, likes, dislikes, loves, and hates.

Key Words:feelings; intuition; fears; impact on others; like; hate; share fears; share excitement;

Key Words:feelings; intuition; fears; impact on others; like; hate; share fears; share excitement;

Green hat

The Green Hat focuses on creativity; the possibilities, alternatives, and new ideas. It's an opportunity to express new concepts and new perceptions.

Key Words: creative thinking; alternative solutions; refine and develop ideas; new perceptions; innovation

Blue hat

The Blue Hat is used to manage the thinking process, to summarize the information, to state the common goals. It's the control mechanism that ensures the Six Thinking Hats guidelines are observed.

Key Words: process; focus; big picture; agenda; mapping the next steps.

TASK:

During the discussion of the conflict you should adopt the attitude and characteristics of the following role:

Blue hat

You are wearing the **Blue hat.**

TO DO:

Define the problem that you are facing and describe it at the beginning of the discussion. Moderate and facilitate the discussion of the situation. Wrap up at the end and try to gather the ideas in decision how to face the conflict.

Having the Blue Hat you have the following role:manage the thinking process, summarize the information and focus on the common goals. You will be the control mechanism that ensures that you are trying to resolve the conflict.

Key Words: process; focus; big picture; agenda; mapping the next steps

Help questions:

What problem are we facing as a group?

How can I best define this problem?

What is my goal and outcome?

What do I seek to achieve by solving this problem?

What is the most effective method of proceeding from this position?

How can I best organize and arrange my thinking to help move me beyond my present circumstances?

Example:

“We have a deadline for an important project that we can’t ignore. However, as teachers, our main goal is to help the students as much as possible. Do you have any ideas how we can find a balance….”

“So, by what has been said so far, we can conclude that it is the best decision to… “

Remember: base your comments on the role (hat) you are having!

Notes:

TASK:

During the discussion of the conflict you should adopt the attitude and characteristics of the following role:

Red hat

You are wearing the **Red hat.**

Having the Red Hat means that you will have the following role: you will rely on your feelings, hunches and intuition. You should express emotions and feelings and share fears, likes, dislikes, loves, and hates, you should cry, yell.

Key Words:feelings; intuition; fears; impact on others; like; hate; share fears; share excitement;

Help questions:

What is my gut telling me about this solution?

What do I feel about the conflict – am I scared, happy, sad?

What are my feelings telling me about the choice I am about to make?

Based on my feelings, is there a better way to go about this?

Intuitively, is this the right solution to this problem?

Example:

"I want to help Tom! I feel so sorry for him!"

"That was an amazing idea, I am excited!"

Remember: base your comments on the role (hat) you are having!

Notes:

TASK:

During the discussion of the conflict you should adopt the attitude and characteristics of the following role:

Black hat

You are wearing the **Black hat.**

Having the Black Hat means that your role is to judge the situation–be the devil's advocate, tell why something may not work. You should spot the difficulties and dangers; where things might go wrong.

Key Words: risks; potential problems; obstacles; downsides; weaknesses

Help questions:

What is the fatal flaw in this idea?

What is the drawback to this way of thinking?

How many ways is this likely to fail?

What are the potential risks and consequences associated with this?

Do I have the necessary resources, skills, and support to pull this off… probably not.

Example:

"Tom came in the worst moment possible! We have a deadline, if we try to multitask we will fail!"

"Even if we succeed applying with the project within the deadline, we might not be approved and it will be a waste!"

Remember: base your comments on the role (hat) you are having!

Notes:

TASK:

During the discussion of the conflict you should adopt the attitude and characteristics of the following role:

Yellow hat

You are wearing the Yellow hat.

Having the Yellow Hat symbolizes brightness and optimism. Under this hat you explore the positive sides of the situation and probe for value and benefit. Face the conflict with optimism and try to encourage the others.

Key Words: best-scenario; benefits; positive thinking; optimism; value and benefits;

Help questions:

How can I best approach this problem?

How can I make this work?

What positive outcomes could result from this action?

What are the long-term benefits of this action?

Example:

"Everything will be fine, don't worry. Let's think positively. I think the best thing to do is…."

Remember: base your comments on the role (hat) you are having!

Notes:

TASK:

During the discussion of the conflict you should adopt the attitude and characteristics of the following role:

Green hat

You are wearing the **Green hat.**

Having the Green Hat allows you to focus on creativity; the possibilities, alternatives, and new ideas. It's an opportunity to express new concepts and new perceptions while facing the conflict. Try to offer innovative and creative methods to solve the problem.

Key Words: creative thinking; alternative solutions; refine and develop ideas; new perceptions; innovation

Help questions:

What alternative possibilities could exist here?

Could this be done in a different way?

How can I look at this problem from a unique perspective?

How can I think outside the box about this?

What if…?

Example:

"Let's try another point of view. What if we try to optimize our resources and do this… and this…."

Remember: base your comments on the role (hat) you are having!

Notes:

TASK:

During the discussion of the conflict you should adopt the attitude and characteristics of the following role:

White hat

You are wearing the **White hat**

TO DO:

Wearing the white hat you have to collect facts, stats, and data that helps you piece together the information it needs to reach logical fact-based solutions. You collect this evidence to help the other thinking hats work through the problem more effectively. You must, however, avoid making conclusions or judgments about the information it has collected.

Having the White Hat you have the following role: Bringing forward stats, facts, and data that can be used to solve the problem. Prioritizing facts over opinions and beliefs.Highlighting gaps in knowledge, perspective, and awareness. Bringing forth logical solutions to the problem at hand. Key Words: process; focus; big picture; agenda; mapping the next steps.

Key words: neutrality, facts, detective, objectivity

Help questions:

What do I know about this problem?

What don't I know about this problem?

What can I learn from this problem?

What more would I like to learn about this problem?

How will I go about acquiring the facts, stats and data that will help me resolve this problem?

What potential solutions exist based on the facts, stats, and data I have collected?

Example:

"So, we just decided that it is better to do…"

Remember: base your comments on the role (hat) you are having!

Notes:

Situation

You are the leader of the scout group. Before leaving for a camping trip, Mario's parents (a new arrival to the scout group) ask to have a private meeting with you to inform you about Mario's situation: the couple is divorcing and he is going through a very delicate phase. They ask you to look after him and try your best to include him in the group.

During the camping, Paolo reports you that Mario has been having hostile attitudes and has been taking funny pictures of younger members of the group, in particular Stefano. The group has found out that Mario has published these pictures on Facebook along with inappropriate comments about Stefano's physical appearances and sexual orientation. He has even created a "hate page" on Facebook with pictures of Stefano with a series of anti gay comments which is becoming increasingly popular at school.

You are facing a delicate position, and you remember about the conversation you had with Mario's parents. How would you solve the conflict?

2.16. References & Links

https://www.understood.org/en/friends-feelings/common-challenges/bullying/difference-between-teasing-and-bullying

https://www.verywellfamily.com/reasons-why-teens-bully-others-460532

https://learnsafe.com/where-does-cyberbullying-happen/

https://www.stopbullying.gov/

http://www.socialeducation.it/

https://www.cyberbullismo.com/grooming/i-cyberpredatori-sessuali/

https://www.lastampa.it/2018/03/16/blogs/skuola/sexting-e-cyberbullismo-caso-su-di-bullismo-in-rete-di-natura-sessuale-1i0R2AIlVr26oD21CdM3sJ/pagina.html

https://www.commissariatodips.it

https://www.linkedin.com/pulse/ottenere-informazioni-preziose-con-mezzi-leciti-mi-innocenzi

www.cyberbullying.org

http://www.age.it/wp-content/uploads/2018/09/CxC-CYBERBULLISMO.pdf

https://www.informagiovani-italia.com/rimedi_cyberbullismo.htm

https://www.laleggepertutti.it/178451_come-comportarsi-in-caso-di-cyberbullismo

https://www.editorialescienza.it/it/scienza/storie-di-bullismo-on-line--che-cos----il-flaming.htm

https://dictionary.cambridge.org/it/dizionario/inglese/sexting