Beware of compromising private photos and videos

- Do NOT take private compromising photos. Somebody can copy, manipulate and distribute them for years on the Internet.
- Do not share photos or videos with unknown people and beware of those who are acquaintances and friends. They can stop being so.
- If somebody asks you to send them this type of photos, tell your parents.
- Never accept blackmail.
- Report any bullying situation.
- When you receive private compromising photos or videos, tell an adult and delete them.
- If you find minors in sexual images, it is child pornography and it is a crime.

**CYBERCONTROL**

Violent cyber harassment in a love relationship that happens in social network or instant messaging.

- Protect your intimacy and privacy, do not provide your partner with your passwords.
- Do NOT tolerate any type of threat, blackmail or aggression.
- There is no argument that justifies violent acts in your relationship, same with cybercontrol.
- Ask for help if you are suffering it and report it.

This material is aimed at young people from SECONDARY SCHOOL

**LOGGING OFF**

Don’t do to others what you wouldn’t like them to do to you!

Logging off is a project from Fundacion MAPFRE aimed at educating young people on the importance of acquiring the right habits for a healthy and responsible use of Information Technologies that leads to a good digital health and identification of risks and dangers of IT misuse.
HOT TO AVOID INTERNET MISUSE?

Protect your digital identity
- Keep your profile private on social networks so that only your friends can see your information.
- Do NOT show personal information (home address, phone number…) on the Internet.
- Be careful with your posts on the Internet. Remember that the Internet has a memory.

Use security methods
- Use safe and complicated passwords (at least 8 characters with upper and lower case letters, numbers, symbols and special characters).
- Use your digital print to avoid phishing (a group of techniques that consist of pretending to be a close person company or entity to obtain data from the victim and get them to do specific actions).
- Alert your contacts in case of identity fraud (another person pretends to be you to obtain some benefit. It can be done by accessing illegally to an account or by creating a new account or profile).
- Cover your webcam when you are not using it and use it only with people you know.
- Install an antivirus in your electronic devices.
- Disconnect the GPS.

Think before clicking
- On the Internet there is inappropriate content for your age and illegal contents that, only by accessing them, you would be committing a crime.
- No matter the content, advise your parents.
- Check that the URL always starts with “https” and that it’s preceded by a locker symbol.
- Check and verify the information. Not everything on the Internet is true.

Do NOT trust unknown people
- On the Internet, not everyone is who they say they are. Do NOT trust.
- Do NOT trust friend requests from unknown people.
- Do NOT be too curious, it can entail risks.

Protect yourself from online games
- Do NOT provide with personal data and keep sessions in private mode.
- If you play online games, do NOT trust people who give you things for free or try to help you.
- Be specially careful with micropayment systems on games.
- Remember that you have to be over 18 years old to participate in online betting. Underage betting is a crime.

Check your apps
- Do NOT trust the free versions.
- Download apps ONLY from official sites.
- Keep your apps updated.
- Check the apps’ permissions before downloading them and assess if it makes sense or not.

Do NOT let your phone control your life
- If you notice that you need to be always online, you are becoming a tech addict and you have a problem.
- Make a difference between use, abuse and addiction.
- Ask for urgent help to parents, teachers or tutors.
- Limit the time you spend online.

Beware of the traps on the Internet
- Do NOT trust bulk messages that come from unknown recipients like spam, misleading advertising or chain messages. Spam is illegal.
- No not participate in viral challenges that can be dangerous for you.
- Check online communities that you are part of. There are communities that discuss inappropriate or dangerous topics.
- Talk to an adult if you know somebody that is being influenced by a dangerous community.

HOW TO AVOID DANGEROUS SITUATIONS?

CYBERBULLYING
To humiliate, assault, insult, isolate or blackmail a classmate intentionally and repeatedly through IT.
- In cyberbullying, the participants are the victim, the aggressor and the witnesses.
- The victim does not relax, no matter the time or the place.
- Cyberbullying expands quickly, it gets seen by more people and cannot be forgotten easily.
- The aggressor can be hidden behind a fake username.

REPORT CYBERBULLYING
If you are a victim, talk to your parents or tutors. Do not be afraid of asking for help. Keep all the evidence.
If you are a witness, do not keep quiet, report it to an adult.

Sexting: Sexual or erotic content footage (photos and/or videos) sent voluntarily through IT.
Sextortion: when somebody threatens another person to send out their compromising photos or videos with sexual content to somebody else or to the public.
Grooming: An adult that pretends to be a minor to become your friend and cheat on you to get something from you, usually with sexual purpose.