OUTPUT 01: 2-Module BEWARE Guide

Data Protection in the Virtual Environment

Editor(s):	**Across Limits Smart Educat. Projects** Angele Giuliano Romeo Bibirigea Melissa Muscat Anca Peptan Juanita Muscat Laura Ditoiu
Responsible Organisation:	AcrossLimits Limited
Version-Status:	V1 - Draft
Date:	22/11/2018-January 2019
Dissemination Level:	Internal

Ersamus+ Programme - Strategic Partnership - AGREEMENT No. **2018-1-RO01-KA205-048881**

cannot be held responsible for any use which may be made of the information contained therein.

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

Chapter 1 Index

Chapter 1

Data Protection in the Virtual Environment

1.1. Generic Introduction

Purpose of this Document

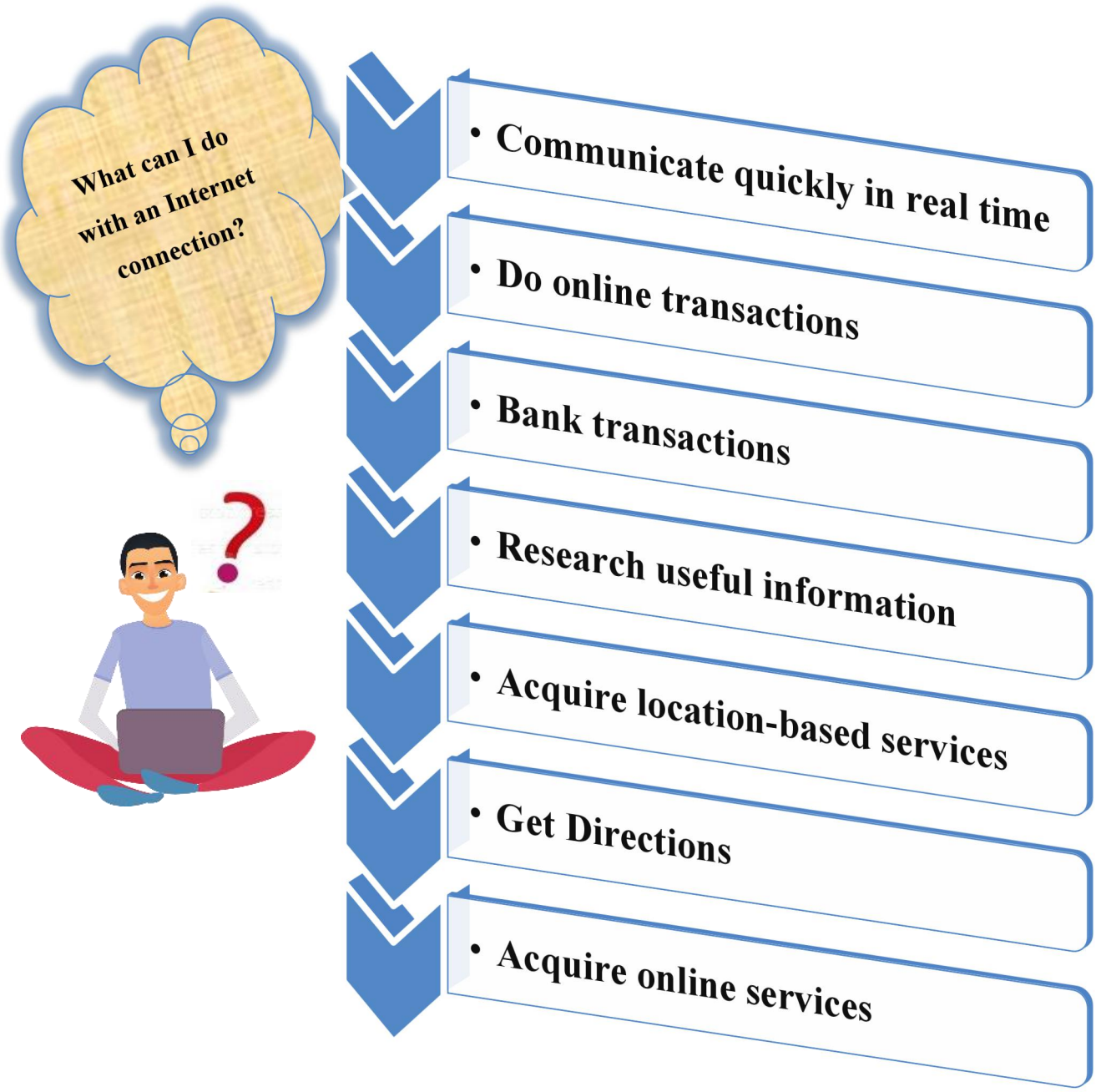
Our lives are predominantly being lived in parallel nowadays - in the real world, where we physically meet with family, friends and workmates, and at the same time online, where we interact with the same or different groups but in a completely different way to our "natural" style of socialization. As 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.

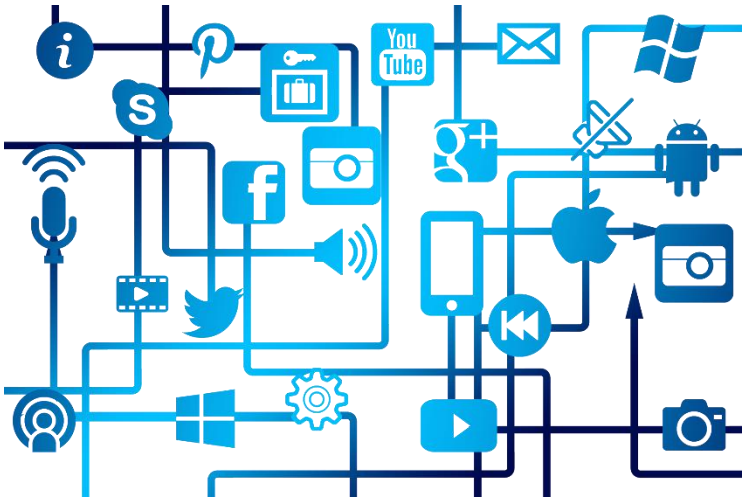
Setting the Scene

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.

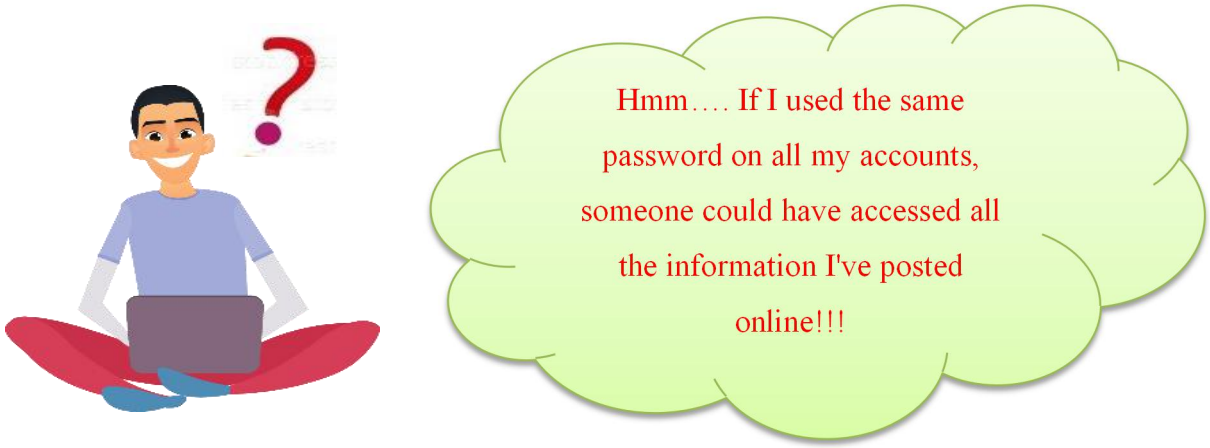
Online Gambling - Gambling games, online casinos and other such apps could lead to gaming addiction, hence jeopardizing the financial situation and general life situation of the gamers.

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



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.

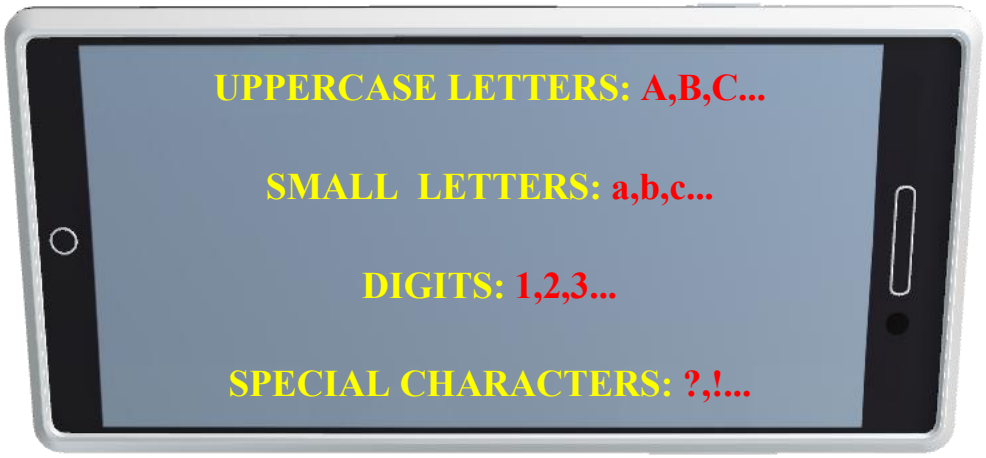
Change your passwords regularly for example every 3 months and do not use the same password for different applications. You must never share your passwords with anyone else, not even your partner, your family members or your best friends.

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

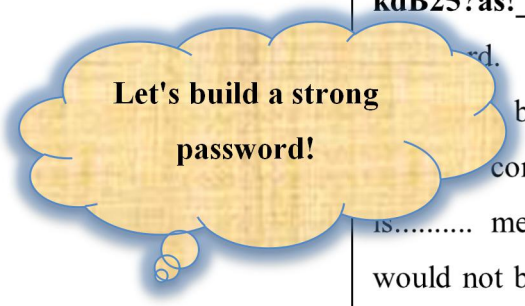
Your password is ... .. **love?** (nice ... no?). **This password can be broken by a hacker in ... 1 second** (according to Kaspersky Secure).

1.3.1. What should a Powerful Password Contain?



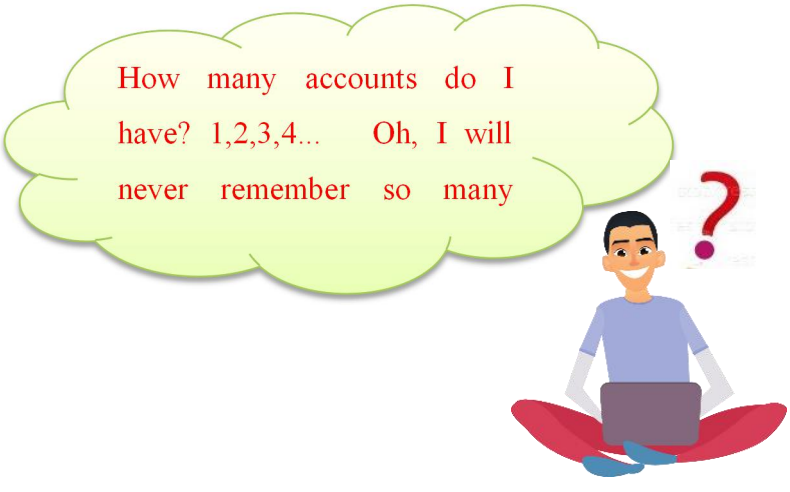
Minimum number of characters: 8

Recommended: 12-14



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

kdB25?as!_S87A



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

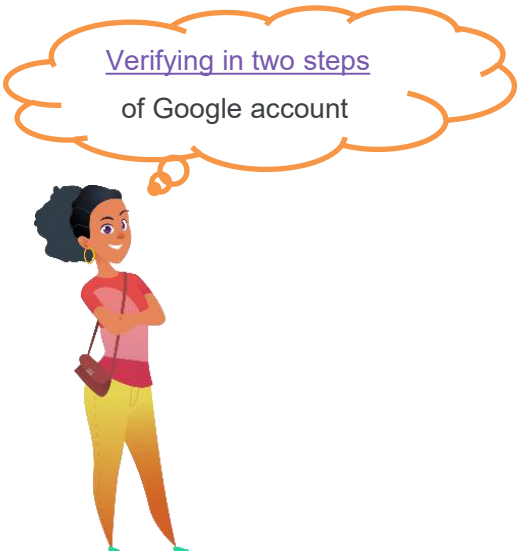
If you do not trust that you can generate a strong password yourself, use one of many available password generating sites: **PWGen**, **LastPass**, **Intuitive Password**, etc. The problem is that you will not be able to remember all of these passwords, and you will have to turn to application password 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.

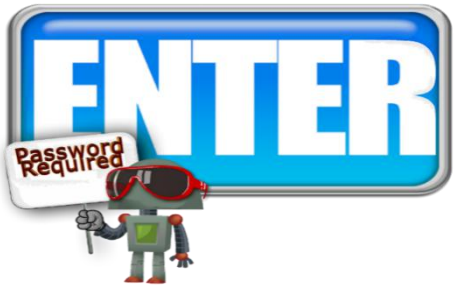
So even if your password has been compromised, the attacker will not be able to access your account without having access to your device**:** phone, email.



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?

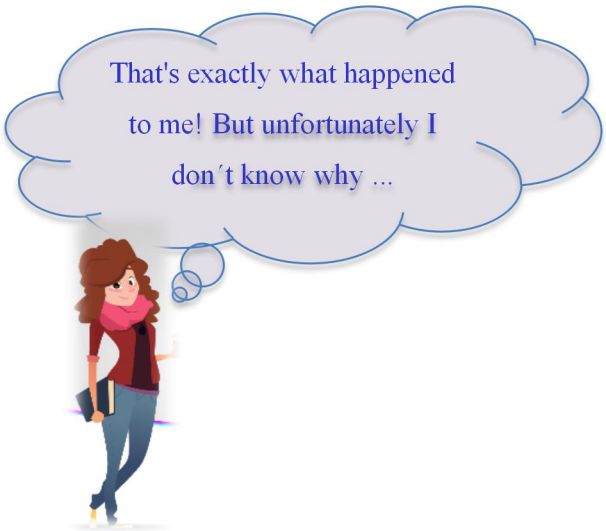
And why couldn't I do that when I go to the toilet or to the bar?

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

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

If you are filling a form and your personal details (address, mobile number, etc) are not

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

Create another email address you only use for online

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

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

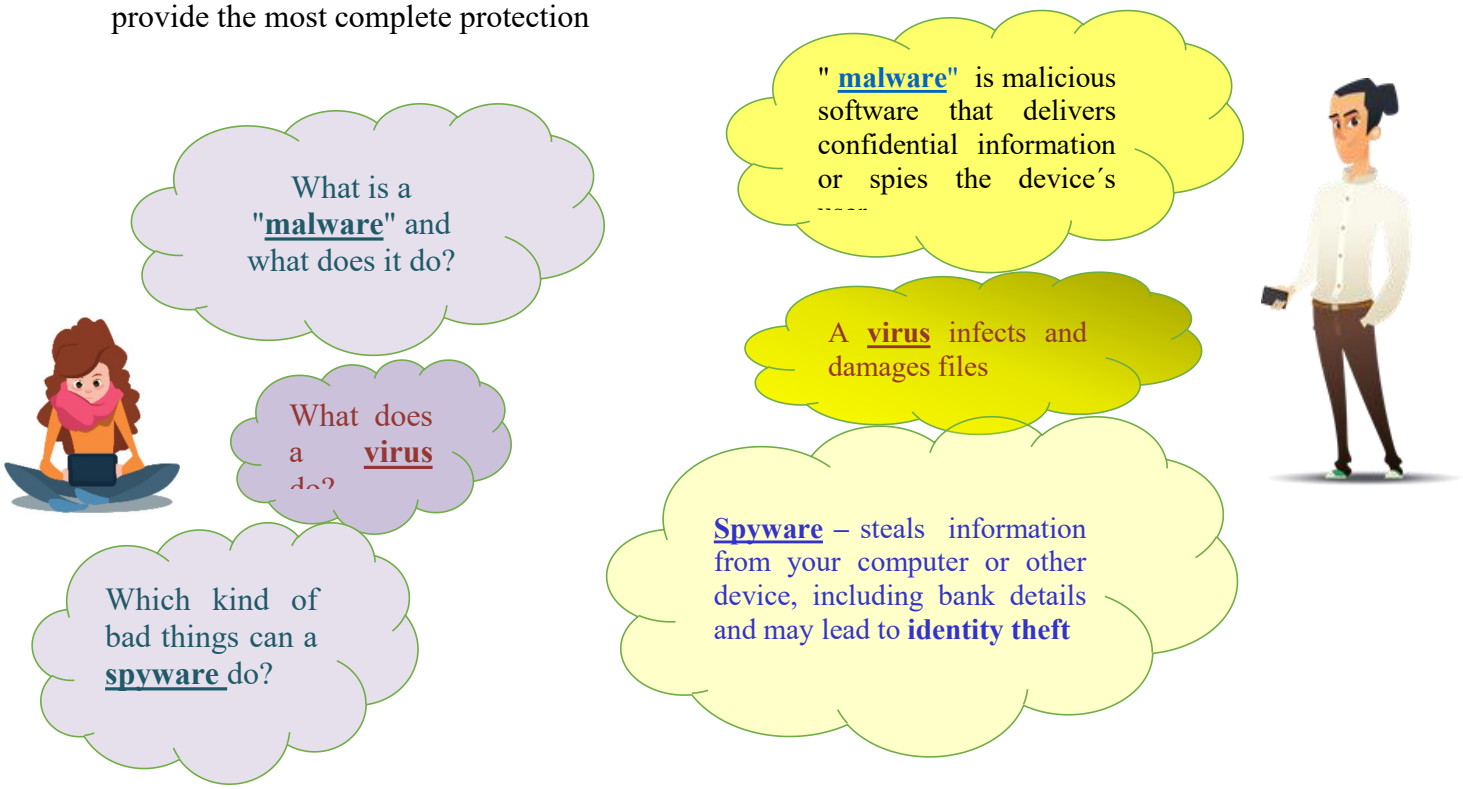
Do not automatically fill in everything on a form!

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

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

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

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

!

- 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???

- 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!!!

What is
viewer?"
good or bad to u

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.

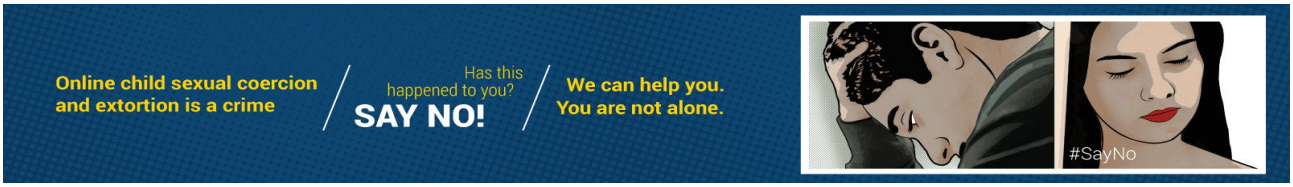
1.5.2. What could possibly go wrong?

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.

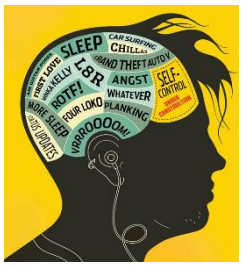
Europol has been running a campaign against online sexual coercion and extorsion. Following is the official page for this public awareness and prevention campaign. It contains also a video in various EU languages:

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



Why does this happen?

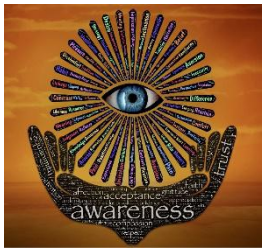
Cyberpsychology, also known as Internet psychology or web psychology is the study of the human mind and behavior and how the culture of technology, specifically virtual reality, and social media affect them. Mainstream research studies focus on the effect of the Internet and cyberspace on the psychology 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



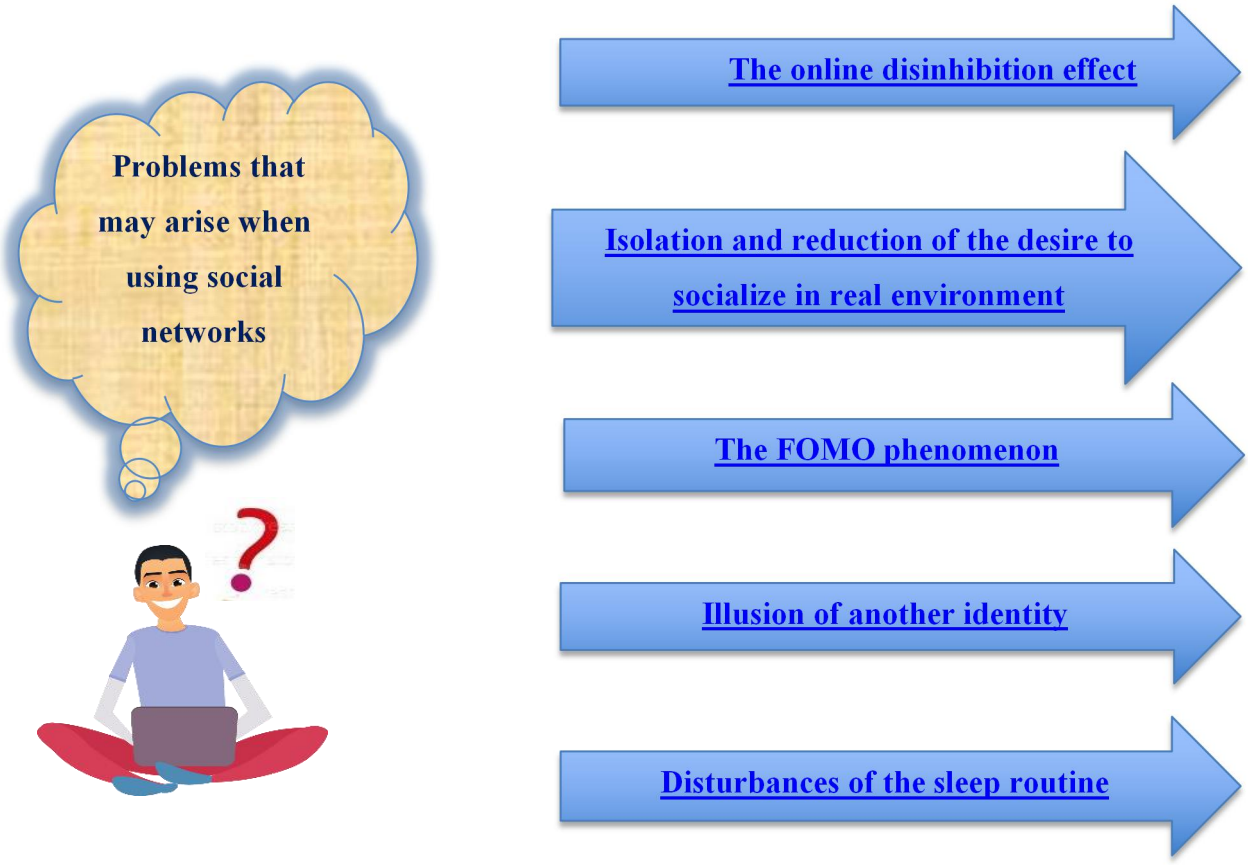
of their need to establish their unique identity. Nowadays, getting feedback from social media connections is the most common way for youths to eventually figure out who they are and what the world expects from them. This is because the first part of the teenage brain to develop is the emotional, impulsive 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

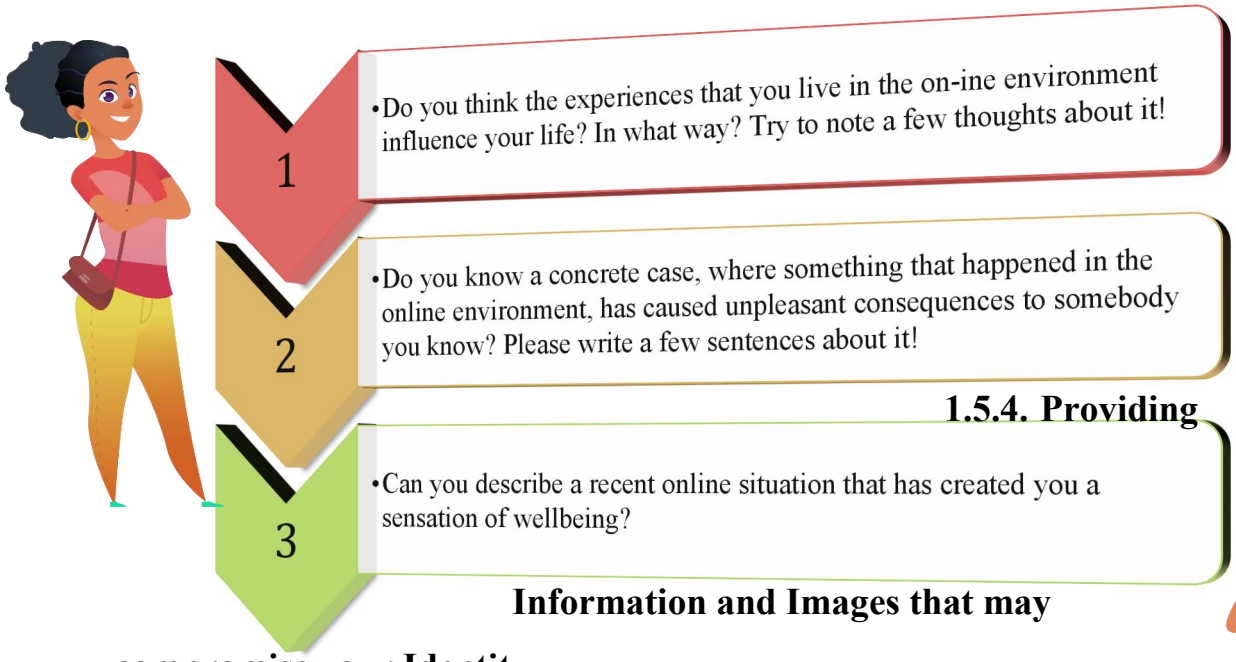
Research shows that people have 2 identities: the real/offline and the virtual/cyber/online. The cyber self is always under construction, psychologically and digitally.

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!



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



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.

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!

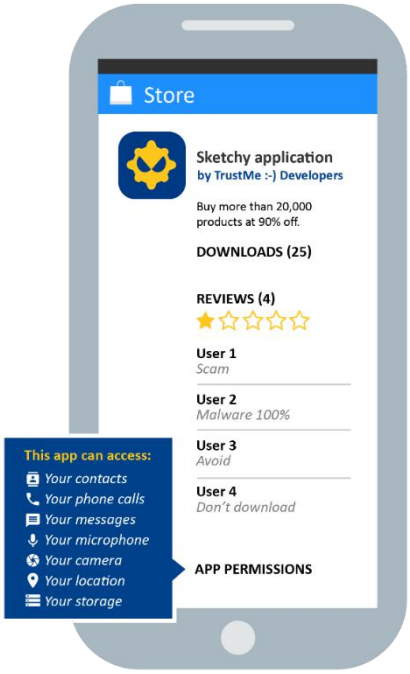
- If there are many updates and content published but little conversations and engaging with members.
- If you receive a request to wire money or reveal sensitive information. A tactic used by scammers.
- If it pushes spam, shares the same link repeatedly in a short period of time or provides misleading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

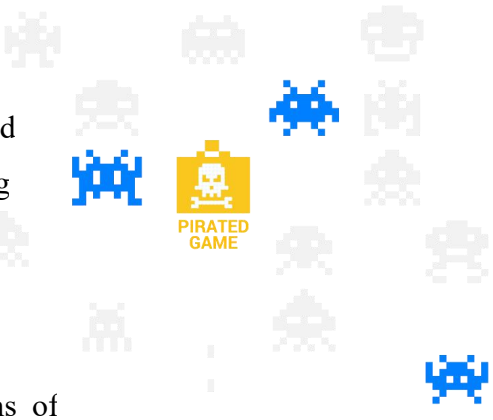
Before downloading an app, Check the F***(ake) Up signs!



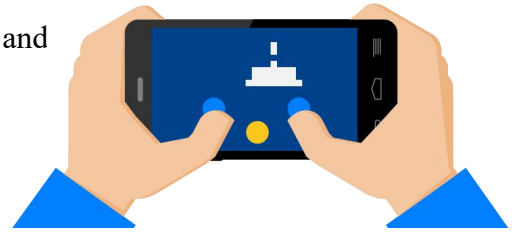
- Be suspicious of apps that promise very high shopping discounts.
- Check the publisher of the app. Criminals can use similar names; so be careful.
- Check other user's reviews and ratings. A fake app will likely have zero reviews while a real app will likely have thousands.
- Check the publish date.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

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

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

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