Collaborative Economy without Barriers

n. 2019-1-IT02-KA204-063246

Guidelines

Risks about the use of online platforms
- How to support the users to prevent dangers

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

Risks about the use of online platforms
- How to support the users to prevent dangers

Start your workshop showing videos or testimonies of people who suffered damage coming from the use of online platforms. From the viewing of this material, which explores problems that may really occur also to them, start a **group discussion** with the learners. Ask if something similar happened to them or to people they know, ask to share with the group their experiece in this field, if they met some problems or dangerous situation using online platforms. Address the group discussion to focus on the risks that could occur by the use of online platforms and a correct behaviour to avoid unpleasant situations.

This video can be an example:

https://www.youtube.com/watch?v=1nzwFsw5Tn0

Prevention - to know how to react

Nothing in the internet is completely private and people online are strangers and they may not to be who they said they are, the users must be aware of this. Inform the users on online safety through educational videos, educational flyers and discussions.
Internet gave rise to many important services accessible to anyone with a connection. One of these important services is digital communication. While this service allowed communication with others through the internet, this also allowed the communication with malicious users. While malicious users often use the internet for personal gain, this may not be limited to financial/material gain. This is especially a concern to most vulnerable individuals as children, disabled people and elders, they are often targets of these malicious users. Common threats to personal safety include: phishing, internet scams, malware, cyberstalking, cyberbullying, online predations and sextortion.

Some example of educational videos about online safety:

https://www.youtube.com/watch?v=HxySrSbSY7o
https://www.youtube.com/watch?v=aMSHtE42mmI
https://www.youtube.com/watch?v=MB5VDIebMd8
https://www.youtube.com/watch?v=GCWBf7WKYyA

Common threats to personal safety in internet

Explain to the users the common threats to personal safety: only by the knowledge of risks and dangers it is possible to recognize and to avoid them.

Phishing is a type of scam where the scammers disguise as a trustworthy source in attempt to obtain private information such as passwords, and credit card information, etc. through the internet. These fake websites are often designed to look identical to their legitimate counterparts to avoid suspicion from the user.

Internet scams are schemes that deceive the user in various ways in attempt to take advantage of them. Internet scams often aim to cheat the victim of personal property directly rather than personal information through false promises, confidence tricks and more.

Malware is malicious software disguised as software designed to collect and transmit private information, such as password, without the user's consent or knowledge. They are often distributed through e-mail, software and files from unofficial locations. Malware is one of the most prevalent security concerns as often it is impossible to determine whether a file is infected, despite the source of the file.

Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization. It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten, embarrass or harass.

Cyberbullying is the use of electronic means such as instant messaging, social media, e-mail and other forms of online communication with the intent to abuse, intimidate, or overpower an individual or group. In a 2012 study of over 11,925 students in the United States, it was indicated that 23% of adolescents reported being a victim of cyber bullying, 30% of which reported experiencing suicidal behavior.

Online predation is the act of engaging an underage minor into inappropriate sexual relationships through the internet. Online predators may attempt to initiate and seduce minors into relationships through the use of chat rooms or internet forums.

Obscene/offensive content, various websites on the internet contain material that some deem offensive, distasteful or explicit, which may often be not of the user's liking. Such websites may include internet, shock sites, hate speech or otherwise inflammatory content. Such content may manifest in many ways, such as pop-up ads and unsuspecting links.

Sextortion, especially via the use of webcams, often this involves a cybercriminal posing as someone else - such as an attractive person - initiating communication of a sexual nature with the victim. The victim is then persuaded to undress in front of a webcam, and may also be persuaded to engage in sexual behaviour, such as masturbation.The video is recorded by the cybercriminal, who then reveals their true intent and demands money or other services (such as more explicit images of the victim, in cases of online predation), threatening to publicly release the video and send it to family members and friends of the victim if they do not comply.

Tips for a safety use of online platforms

- Choose strong passwords, often people tend to choose easy ones to remember which are also easy for cyber thieves to guess. Select strong passwords that are harder for cybercriminals to demystify.
- Keep your profile in private mode and Keep your privacy settings on to take charge of your information.
- Keep personal information limited, unknown people do not have to handle your private information as your home address, your personal relationship status, your documents... They do need to know about your expertise and professional background, and how to get in touch with you.
- Choose an appropriate picture as photo profile.
- Do not send any private/personal pictures from yourself as well as others.
- Do not accept friendship requests (e.g. Facebook) from people that you do not know in the real life. In some cases, as in collaborative economy, you should communicate with unknown people but be aware that people with who you are talking online is not your friend.
- Keep your friend list private (e.g. Facebook).
- Do not click any link to download, do not download apps that look suspicious or come from a site you do not trust.
- Do not open any attachment excluding pdf documents.
- Be careful about what you post, any comment or image you post online may stay online forever because removing the original does not remove any copies that other people made. There is no way for you to “take back” a remark you wish you had not made. Do not put anything online that you wouldn’t want your mom or a prospective employer to see.
- Limited using: estabilish a time to use online platforms to avoid to loose the perception of time and to spend all the day online.
- Be careful who you meet online, people you meet online are not always who they claim to be. Indeed, they may not even be real.
- To meet unknown people could be dangerous, If you have this necessity, e.g. to exchange/buy/sell products, ask to a trusted adult to come with you. Meet new people only in pubblic places and tell to somebody where are you going and with who.
- Be kind and respect other people and viewpoints different from yours. Remember that communication and even more virtual communication is easy to misunderstand: keep calm and avoid conflicts.
- If someone approaches you online and makes you unconfortable stop communication with them and tell it to a trusted adult (educators, volunteers, parents).
- Think before to click!

Tips for educators and social workers to support users in the use of online platforms

- Because every people is different and so also their needs, **it is not possible to use the same instruction and methodologies for everybody.** Educators and social workers must be careful to evaluate those who can use online platforms autonomously after a good preparation and those who can use online platforms only with a properly support of educators, volunteers, friends, family.
- It is essencial to **monitor** the users, to guide them to assume correct behaviours for a safety use of online platforms and to face on time with problems that may occur.
- For an effective learning it is important to estabilish a connection between educators/ volunteers and users and to **build trust**, so the users will feel confortable asking questions and they will be aware that they can count on this person in case they need any help.
- **Problem solving** - Role of the educators is also to explain to the users what they did wrong, be sure that they really understood and agree with you, fix it together and explain how to avoid it next time.
- Could be necessary to **limit/estabilish the time of use** of online platforms with the users to avoid dependence on internet usage.
- Use **filters** to limit or lock the files or web pages that the users can access.
- **Password and username** are very easy to forget, register the data of the users in a document so that in case they will forget their credentials you can find them without the need to create a new account.

Misunderstanding due to the communication can be one of the main causes of conflict that can occur using online platforms, this subject is treated in the Guidelines “How to structure learning sessions about communication”.
See also the Guidelines “How to instruct the learners in writing a profile in collaborative economy platform and how to manage that.”

This guideline was realized during the Joint-short term staff training event: Mutual learning for the best support. The training event was held in Palermo on 04.02.2020 -08.02.2020. The guideline aims to support the work of educators and social workers in guiding the adult learners with disability in participating to collaborative economy. It is a product of the Project Collaborative Economy without Barriers – CEB, a Strategic Partnership for the exchange of good practices in the field of adult education, Co-funded by the Erasmus+ Programme of the European Union.

All the guidelines realized during the Project Collaborative Economy without Barriers – CEB and informations about the project and its activities are published in the following web-site: https://partnershipceb.blogspot.com

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein"

Sitography

https://usa.kaspersky.com/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online
https://en.wikipedia.org/wiki/Internet_safety
https://www.youtube.com/watch?v=MB5VDIebMd8
https://www.youtube.com/watch?v=HxySrSbSY7o
https://www.youtube.com/watch?v=aMSHtE42mmI
https://www.youtube.com/watch?v=GCWBf7WKYyA

CEB

Collaborative Economy without Barriers

The partnership:

Associazione Uniamoci Onlus (Italy) - Coordinator
Diakonisches Werk Bremen e.V. (Germany)
Centro Social e Paroquial Santos Martires (Portugal)
Fundatia Crestina Diakonia Filiala Sfantu Gheorghe (Romania)
Go Green Skopje (Macedonia).

facebook

Contacts:

ASSOCIAZIONE UNIAMOCI ONLUS
via E. Giafar n° 36, 90124 Palermo
Tel. 0919765893
www.uniamocionlus.com
www.social-uniamocionlus.org
info@uniamocionlus.com

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

ASSOCIAZIONE UNIAMOCI ONLUS

Diakonie Bremen

Diakonia
Fundaţia Creştină Diakonia
Serviciul Caritativ al Eparhiei Reformate din Ardeal

santos mártires
centro social paroquial

GG