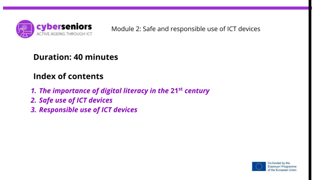
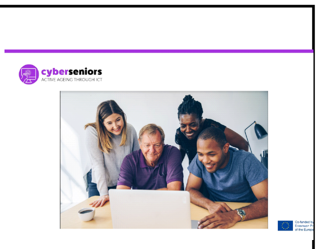
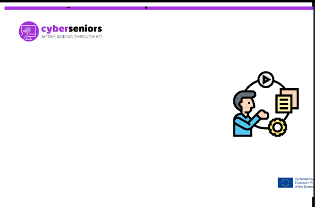
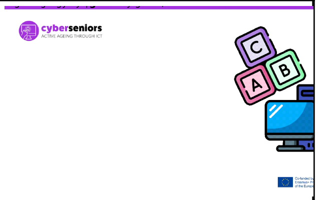
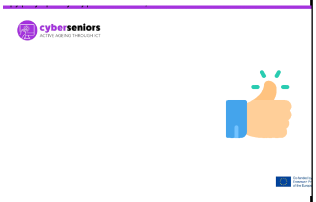
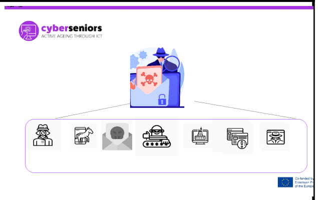
Training guide

Module 2/ Safe and responsible use of ICT devices

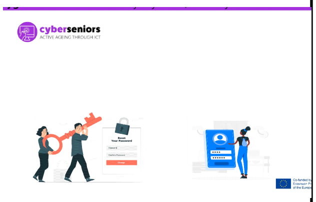
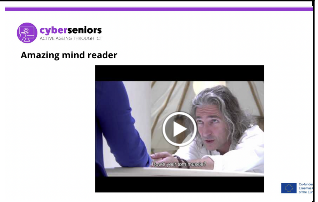
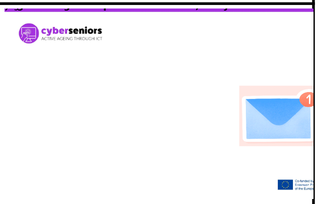
Before the session
● Have all the necessary material ready (computer, presentation, pendrive, etc ...) ● Prepare your presentation well ● Have a positive and motivating attitude ● Be punctual

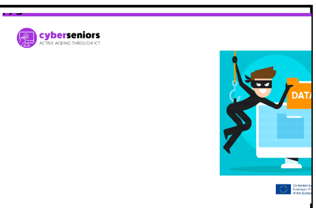
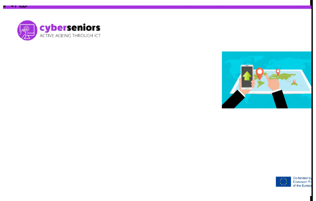
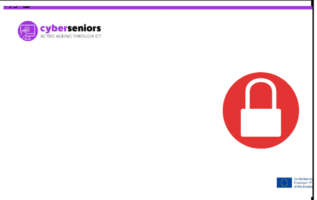
During the training		
Duration	**Main session - 40 minutes**	Relevant presentation slide
2 mins	During the session: ● Welcome your audience and introduce yourself to create a good atmosphere. ● Be aware of timekeeping at all times so that you can cover all the material. ● Leave some time at the end to clarify doubts and questions ● Act with empathy, patience and closeness ● Try to make sure that your audience follows your explanations	cyberseniors ACTIVE AGEING THROUGH ICT Co-funded by the Erasmus+ Programme of the European Union CIBER VOLUNTARIOS.org SYNTHESIS Vienna Association of Education Volunteers Age& Oppo
3 mins	We will explain that Cyberseniors is a project co-funded by the European Commission through the Erasmus+ Program, with the main objective of creating training resources for people over 55 years of age, on how to manage a smartphone, and useful applications for an active aging and a higher autonomy. We remind that all info, as well as these resources, are available at www.ciberseniors.org We will explain the index of today's session and also inform about the content of the 4 modules (4 hours training in total) 1. Introduction to the use of smartphone/tablet 2. Safe and responsible use of Information and Communication Technologies (ICT) 3. ICT applications for mobile phones and tablets I (leisure, health, communication) 4. ICT applications for mobile phones and tablets II (banking, daily needs and accessibility, public administration	cyberseniors ACTIVE AGEING THROUGH ICT Module 2: Safe and responsible use of ICT devices **Duration: 40 minutes** **Index of contents** *1. The importance of digital literacy in the 21st century* *2. Safe use of ICT devices* *3. Responsible use of ICT devices* Co-funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this document 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

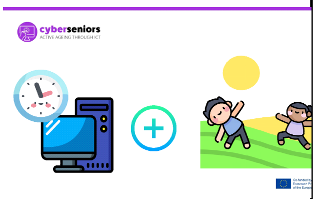
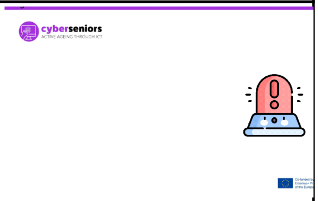
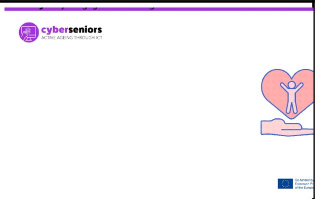
10 mins	The evolution of digital technology has transformed the way we interact with other people and how we carry out our daily activities. Digital literacy is a fundamental skill for all of us, in order to learn how to navigate in the digitized contemporary world and to adapt to the changing needs.	
	- Contemporary daily needs - Email - Virtual communication - Digital transactions - Phone reminders	
	Digital literacy refers to: - The required skills to achieve digital competences; - The safe and critical use of information and communication technologies (ICTs) to work, leisure, learning and communicate (Eurostat Glossary, 2019); - The familiarity with the basics of digital security and the use of authorized content.	
	Digital literacy has these benefits: - It opens up a world of opportunities; - It unites people; - It allows us to do things remotely (Very important with COVID19) - It improves our skills and it enables lifelong learning; - It promotes independence and empowerment;	
15 mins	These are some of the most common types of threats, intended to **impersonate** another person in order to steal data or alter the data of a server. Phishing techniques also use identity fraud to make us think that we are sending our data to a trusted website when in fact the hacker is receiving it, e.g. impersonating through facebook to steal our password. **Trojan** is software masked as beneficial and it pretends that we install it in order to gain access to our data or to turn our computer into a member of a botnet. It can be disguised as anything, office suites, antivirus, banking software, etc. For this reason, it is essential that we distrust any software that we install. We should install softwares only from reliable sources (app stores) and we should check every software that we install with an antivirus.	

	SPAM: the concept of spam is very broad and it covers all unwanted communication with someone that can become nonexistent and be repeated or not. As a general rule, it is produced by email, but it can be produced by any other means, whatsapp, sms, phone call, etc. The purpose can be to get website information, data theft, installation of malicious software, etc. **Social engineering** exploits our weakness as humans to trust others and thus obtain the necessary information for an attack. For example... a 'support' call that asks us for a service password to solve a problem. Social engineering is also considered to be the study of of a user public information (social networks, personal websites, etc.) in order to obtain relevant information for an attack... e.g. We publish the name of our pet on Facebook with universal visibility. A supposed attacker will add this information to the list of passwords that he/she will try to enter the accounts. **Phishing**: Phishing is a technique that leads to the installation of malware, theft of data or money through email messages, websites, phone calls (vishing) or SMS (smishing) that seem legitimate in appearance and context, but that could bring us to a website where they are going to steal data, facilitate the installation of malware, or steal money from our credit cards, among other actions. **Adware**: is a software that shows us ads in our applications or web pages that we visit in order to generate profit for the malware creator through our clicks on the ads. **Spyware**: it is a software that spies on our actions on our device. If our device has multimedia functions or location sensors, it can spy on that information, activate cameras or microphones or access our location on the mobile, etc.	

	Half of seniors don't use the password feature on at least one of their internet-enabled devices, creating the possibility that it could be picked up by anyone. Lock all your devices including computer, tablet and smartphone with strong passwords. That will keep prying eyes out and it will be a defense in case your devices are lost or stolen. How often do you need to change passwords? Unless you become aware of a password breach, there is no need to change your passwords often if each one is a strong and unique password. However, if you think one of your accounts has been hacked, please change your password immediately.	
	When creating social media posts, you can choose privacy settings to select which audience will see your post. It could be just the friends you added on the social network, it could be a public post to anyone, or it could be a private post just for you. You can also specify or not specify your location. Make sure your private information is not shared (passwords, phone number, email, etc.) *We will put the video of the next slide to reinforce the danger of free access to our information on social networks, for example.	
	This video shows some of the threats we have seen before and how some cybercriminals act	 Amazing mind reader
	During your communication via social networks, messaging and email, you should be careful not to click on links sent to you by an unknown person. Cybercriminals can impersonate, for example, Facebook employees or Instagram's security service. Do not trust those messages, if you receive them through a normal chat, a post or from a normal Facebook page. Safety messages will be sent to you via notifications or will be available in settings. Employees of social networks will never ask you for your password or private information.	

	If friends or family ask you to help them in an emergency, always call to speak with them personally and to confirm if they really sent the message. Otherwise, those messages may be from cyber criminals. They may create a profile that will be identical to your friend's or family member's profile and try to get money from you.	
	You can use Google's "Find My Phone" tool, if you are logged into your Google (gmail) account on your phone. First, you must allow Google to use your location data, device information, and connection events to locate your devices and accessories. Your device's location may not always be accurate, but you'll see a map of your phone's current location. Data related to the charge level and connection to the mobile network will also be available. You will have several options: - Set the alarm on your phone. The device will ring for five minutes even if the phone is in silent mode. - Lock your phone and sign out of your Google account. You can also display a text message on the phone screen. - Wipe device data by resetting to factory settings. After that, you will no longer be able to monitor your device.	
	Tips - Secure access to your accounts. - Think before acting. - When in doubt, check. - Share carefully. - Use security software. - Configure security of your browser. - Use antivirus (also on mobile). - Sign out. - Ask for help.	

The European Commission support for the production of this document 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

5 mins	- It is necessary to maintain a mental and physical balance. - Manage your interactions with digital tools - Digital wellbeing influences our general well being and vice versa. The best suggestion is to find a balance between both “worlds”, in order to get the best enrichment and positive benefits in every area, reducing the risks of an excessive use of digital tools that, as we have seen, could affect us in different ways. Use technology to interact with the physical world and other people in an active way.	
	These are some consequences of technology abuse	
	- Understand and control your technology habits - Set limits - Manage your connections better - Take breaks regularly - Get a good night's sleep and rest, avoid using technology before going to sleep	
5 mins.	**CONCLUSION**	
	We will leave some time until the end of the session to resolve doubts or concerns about what was seen in today's session. We will appreciate their participation and we encourage them to practice at home so as not to forget what they have learned today.	

THANK YOU SO MUCH