DISK | Digital Immigrants Survival Kit

Training Content Framework
11 Privacy and Device Safety

Description of the Training Module 11

Training Content Framework: 11 Privacy and device safety

Module title	11. Privacy and device safety (Safety, digital identity)
Notional Learning time	Approx. 6 hours
Description of the module	The module will provide strategies and modalities to protect the digital identity of users. Participants will gain insights in recognising digital threats, preventing fraud, identity theft and other cybercrimes. The module will explore the concept of digital identity and illustrate basic strategies to protect it in the digital environments.
Learning objectives	Course participants will learn to: • Be aware of own digital identity • Recognize digital threats, preventing fraud, identity theft and other cyber attacks • Implement successful action to avoid data breaches in digital environments

Steps	The steps to accomplish the learning objectives are the following:
	• Carry out the pre-module self-evaluation mandala to assess the level of digital competences according to the Likert scale model.
	  • Read basic content and follow the instructions about:
	  • Digital threats
	  • Device protection strategies and tutorials (the smartphone screen locks)
	  • Digital safety
	• Best practices when browsing on the different digital environments
	• Carry out practical tasks. Learners will be given real-life situations to use digital tools adequately, protecting own devices and personal identity
	• Carry out intermediate assignments (quizzes, multiple choices, T/F)
	• Search and familiarize with key words in the glossary
	• Carry out the final self-evaluation test at the end of the module
	• Carry out the final self-evaluation Mandala and compare it with the previous one. The aim is visualizing the learning process after the module completion.

DISK | Digital Immigrants Survival Kit

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

Material	
Learning content	Users will learn the existing regulations concerning the illicit appropriation of identity, they will go through possible attacks from fraudsters and preventive solutions, how to implement successful actions to avoid breaches in the digital environment. The learning content will be presented through: • H5p (interactive presentation, videos, Memory card game) • Moodle Forums • Moodle Book resource • Moodle Glossary resource • Exe-learning (self-assessment in HTML5 format) • External links
Learning content type in moodle	Learning contents will be presented as follows: 1. Forum to share content and interact with other participants 2. H5P interactive presentations to give an overview and complete intermediate tasks, to illustrate how to integrate multimedia in own created content 3. H5p interactive videos to integrate varied content and provide insights 4. H5P activities: quiz, drag and drop, T/F, choose the correct statements integrated in presentations and videos 5. Links and webpages to share external resources/ insights 6. Glossary with key words 7. exe-learning self-assessment to check the module comprehension and key-concepts
Activity/Task	Students will be completing the following activities: 1. Read the theoretical background concerning digital theft and identity theft 2. Use the pre-module self-evaluation Mandala and self-assess own digital competences according to the module 3. Check key words in the glossary 4. Read the H5P presentations, answer to quizzes, check results 5. Complete the assigned practical activities on H5P based on real-life situations 6. Share your ideas and best solutions with other users of the platform 7. Read external reading materials and theory-related games 8. Carry out the final self-evaluation test at the end of the module 9. Use the final self-evaluation Mandala to self-assess the new digital competences acquired after the module
External resources	OER links, videos, images, pdf

Evaluation	Knowledge will be assessed through intermediate interactive activities on H5P and a final self-evaluation will be inserted at the end of the module. Learners will be asked to self-evaluate their own digital competences at the beginning and at the end the module through the self-evaluation Mandala. It is personal but could also be shared with the teacher/educator/tutor if needed.		
Learning outcomes in terms of competence	Knowledge	Skills	Attitudes
	To know different way to protect own digital identity and device from digital threats and cybercrimes	To distinguish and recognize digital threats and avoid dangers linked to improper uses of personal devices.	To apply different digital safety measures and strategies in order to protect personal data and information.
	To protect digital identities and devices from digital threats and dangers of the Internets.		
Evaluation content	The final exe-learning file contains 20 questions which are all multiple choice on the topics of the module.		