



Co-funded by
the European Union



REMCREAD

Empowering Refugee & Migrant Women
through Creative Methods and Digital Literacy

MODULE 3: Safety and privacy online LESSON PLAN

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Project no. 2023-1-PL01-KA220-ADU-000156610

Project website <https://www.remcreadwomen.eu/>



Module 3. Security and privacy on the web

Introduction

The 'Online Safety and Privacy' module has been developed as an interactive online resource, available at: [Safety and Privacy Online](#). These resources can be used in a variety of ways - as a presentation during a classroom session, as part of an e-learning course or in a blended-learning format, combining online and offline work.

The aim of the module is to raise participants' awareness of data protection, safe use of social media and minimising risks associated with online activity. The materials guide participants step-by-step from understanding the essence of online security, through practical skills (including creating strong passwords, configuring privacy settings, using 2FA) to consciously publishing content and responding to privacy breaches.

The structure of the module is based on a lesson plan that includes:

- an introduction to security and privacy,
- risks associated with social media (data theft, phishing, cyberstalking, spoofing, addiction),
- the principles of secure logging on and use of public Wi-Fi networks,
- the consequences of publishing personal data, photos and location information,
- a case study and group exercises,
- a summary and additional resources and tools.

The online resources include videos, graphics, links to external resources and described exercises that can be completed individually or in groups. The guide also provides guidance on how to conduct discussions and case studies to engage participants and help them transfer the knowledge they have gained to their own online experiences.

Thanks to the flexible format, the material can be delivered in both a full version (approximately 120 minutes) and a shortened version to suit the time capacity of the group.

The educator decides which elements to include, taking into account the needs and competence level of the participants.



Safety and Privacy online

Digital security competency matrix for a person active in social media

Competency area	Knowledge	Skills	Attitudes
Password management	- Principles for creating strong passwords - The role of password managers - The importance of 2FA	- Creating and changing strong passwords - Configuration of 2FA on different platforms - Supporting the password manager	- Taking care to use various passwords to different accounts - Trusting password management tools - Caution in sharing passwords
Awareness of phishing and social engineering	- Types of phishing attacks - Social engineering techniques used by cybercriminals	- Recognizing suspicious messages and sites - Reporting phishing - Protecting personal information	- Critical approach to received messages - Caution in providing data - Alertness to unusual situations
Security of devices	- The role of system updates - The importance of antivirus and firewall - Threats associated with physical access to devices	- Installing and configuring antivirus - Regular updating of software - Securing devices	- Keeping software up to date - Awareness of the risks associated with lack of security - Responsibility for one's own devices
Data and privacy management	- Privacy settings on platforms - Data protection - RODO (GDPR) regulations	- Configure privacy settings - Limiting the visibility of personal information - Sharing information securely	- Respect for your own and others' privacy - Responsibility for the data being processed - Legal awareness related to data protection



Safe use of networks	- The dangers of public Wi-Fi networks - Features and benefits of using a VPN	- VPN configuration - Using Wi-Fi networks safely - Avoiding risky Internet connections	- Caution when using public networks - Being proactive in securing connections - Awareness of online threats
Account and content management	- Account monitoring tools - The role of privacy policies in social media	- Regular review and analysis of account activity - Secure publication of content	- Responsibility for published content - Attention to compliance with privacy policies - Being proactive in monitoring activity

Module 3. Security and privacy on the web

Learning outcomes:

Workshop participants:

- understand why online privacy and security are important;
- are able to create strong passwords and use two-factor authentication;
- are able to set appropriate levels of privacy on their social profiles;
- are aware of the risks involved in publishing personal data, photos and locations;
- know how to use public Wi-Fi networks and strange devices safely;
- know how to respond in the event of a breach of privacy or account takeover;
- are able to assess what content is safe to post on social media.

Duration: 120 minutes

Activities	Objective	Methodological notes	Materials	Time	Other resources / link to resources
1. Introduction: Why is online privacy important?	Raising awareness of online risks and their consequences.	Brief introduction by the trainer + real-life examples	Content from https://sites.google.com/view/safety-and-privacy-remcread-en - Magda's story, Christopher, coach examples.	15 min	https://sites.google.com/view/safety-and-privacy-remcread-en

2. Strong passwords and 2FA	Participants will learn how to create strong passwords and understand the importance of two-factor authentication.	Step-by-step demonstration Suggested footage that is in English can be translated using the settings in Youtube. Suggested material in the form of web pages can be translated into any language using a translator in a browser such as Chrome. For the best translation it is suggested to use the page prepared in the project in English.	Whiteboard/flipchart, marker, mobile apps	15 min	Instructions for creating strong passwords and configuring 2FA ▶ How to protect... ▶ What Is Two-F... What is Authentication Two-Factor Authentication 2FA: Secure Your Digital Life What is Password Manager Do I need it
3. Profile privacy settings	Participants independently check and change their account settings.	Individual work with phone/laptop + trainer support.	Internet access, YouTube instructions	20 min	How to configure privacy in Instagram
4. Informed sharing of content	Participants are able to distinguish which content is safe to publish.	Guided discussion, analysis of examples.	Content from https://sites.google.com/view/safety-and-privacy-remcread-en	15 min	Privacy and Social Media

5. Secure logging on and use of Wi-Fi	Participants know the risks associated with public Wi-Fi and how to avoid them.	Presentation + questions to the group	Content from https://sites.google.com/view/safety-and-privacy-remcread-en	15 min	Cybersecurity Basics - Educate and protect yourself
6. What to do in the event of a privacy breach?	Participants know the steps to take after an account has been taken over.	Discussion, analysis of procedures	Descriptions of procedures (Facebook, Instagram, Twitter X)	15 min	https://help.instagram.com/
7. Case study: Maria and the safety of refugee women	Reflection on the safety of vulnerable users.	Group work + presentation of conclusions	Maria's case report https://sites.google.com/view/safety-and-privacy-remcread-en	20 min	
8. Summary and questions	Highlighting key principles and addressing concerns.	Open questions, collection of conclusions		5 min	