information matters

Training Programme for Online Courses

Module 9

Media Literacy & Privacy

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Contents

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Description for online Lesson

Welcome to the module on media literacy and privacy. In this lesson, we will explore the importance of protecting personal data and maintaining online privacy, particularly for elderly individuals. By the end of this lesson, you will have a deeper understanding of privacy issues in the digital age and be equipped with practical strategies to safeguard your personal information.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Let us see some main definition and examples

- **Personal data** is any information that can be used to identify an individual, therefore refers to any information that directly or indirectly relates to an individual. It includes details such as your name, address, phone number, email, birthdate, and even more sensitive information like your financial records or medical history. Personal data is valuable and should be kept private to protect yourself from potential misuse or exploitation.
  It is essential to protect the privacy of these data from being shared or accessed by unauthorised parties, as this can lead to identity theft or other forms of cybercrime. To prevent leaking personal data, we need to understand how to use privacy settings on social media and other online platforms, avoid sharing sensitive information over unsecured networks, and use strong passwords and other security measures to protect their accounts.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

- **Online privacy** refers to the ability to control and safeguard your personal information while using the internet. It involves keeping your personal data secure, limiting the amount of information you share online, and being aware of who can access your online activities. By understanding and practising online privacy, you can maintain greater control over your digital identity and protect yourself from online threats like identity theft, scams, or unauthorised surveillance.
- **Your digital footprint** is the trail of information you leave behind while using digital devices and the internet. It encompasses your online activities, including the websites you visit, the social media posts you make, the comments you leave, and the images or videos you share. Your digital footprint can have long-term consequences and can be used by others to track your online behaviour, influence decisions, or even determine your credibility. Understanding your digital footprint is essential to maintain a positive online reputation and protect your privacy.

Overall, it is important for elderly individuals to be proactive in protecting their privacy in the digital environment. By staying informed, using secure practices, and being mindful of our online activities, we can minimise potential risks and achieve a safer online experience.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

What does online safety mean for elderly people?

Online privacy and applying a range of safety initiatives regarding personal data protection and personal information means:

- To know and apply basic rules and principles for safety, protecting privacy and personal information;
- To apply privacy settings and permissions such as cookies, to have an awareness of tracking tools, to be aware of your digital footprint;
- To acquire awareness of strategies and tools currently used to tracking, spying, and intruding the private sphere.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

How can you train your elderly participants about media literacy and privacy?

- You can find useful contents and further links related to media literacy and privacy in the training program.
- Apply activities planned for elderly learners to support their awareness about privacy. By working through and implementing these training activities, you can motivate and support your participants to collect and develop the desired skills and competencies in the area of media literacy and privacy. The exercises offer opportunities to expand knowledge in the following 3 areas:
  - How to keep and use passwords safely?
  - Keep personal information safe – stories about privacy
  - Online banking without fear
- It may be that your participants have previously used different, not so appropriate rules for dealing with passwords. They need more patience and time to work through that maybe they should change their practices.
- Spend enough time practising a method that your participants can use with confidence.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

- Elderly people are often afraid of online banking, since this approach seems to be too unsafe for them. So our goal is in the first step to testify and get closer to their fears so that we can understand under which circumstances we should work.
- If you know the circumstances of your participants, you can adapt the stories and further activities accordingly.
- Motivate your learners to make a summary of the safety rules as a reminder for their future online activities. Produce this rule in an appealing way and distribute under your participants.

Congratulations on completing Module 9 – Media Literacy and privacy!

Remember, by staying informed, using secure practices, and being mindful of your online activities, you can minimise potential risks and achieve a safer online experience. Utilise the provided resources to support your participants to enhance their knowledge and continue their journey towards becoming media literate and privacy-conscious. Stay vigilant, stay safe, and enjoy the digital world responsibly.

We advise you to continue with lesson 10. Good luck!

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Introduction

Personal data is any information that can be used to identify an individual. It is essential to protect the privacy of these data from being shared or accessed by unauthorised parties, as this can lead to identity theft or other forms of cybercrime. To prevent leaking personal data, elders need to understand how to use privacy settings on social media and other online platforms, avoid sharing sensitive information over unsecured networks, and use strong passwords and other security measures to protect their accounts.

Overall, it is important for older individuals to be proactive in protecting their privacy in the digital environment. By staying informed, using secure practices, and being mindful of their online activities, they can minimise potential risks and achieve a safer online experience.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Learning Outcomes

Participants will be able to understand the importance of privacy and discuss possible vulnerabilities in the use of the internet and digital devices. They will also gain learning about protecting and sharing personal information responsibly. At the societal level, they will mature an increased awareness of the impact of disinformation in the public sphere.

Main keywords

Personal data, online privacy, digital footprint, Internet hygiene, Precautionary measures.

Subjects

Online privacy and applying a range of safety initiatives regarding personal data protection and personal information:

- Basic rules and principles for safety, protecting privacy and personal information;
- Privacy Settings and permissions such as cookies, awareness of tracking tools, digital footprint;
- Awareness of strategies and tools currently used to tracking, spying, and intruding the private sphere.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Terms and definitions:

- **Personal data:** Personal data refers to any information that directly or indirectly relates to an individual. It includes details such as your name, address, phone number, email, birthdate, and even more sensitive information like your financial records or medical history. Personal data is valuable and should be kept private to protect yourself from potential misuse or exploitation.
- **Online privacy:** Online privacy refers to the ability to control and safeguard your personal information while using the internet. It involves keeping your personal data secure, limiting the amount of information you share online, and being aware of who can access your online activities. By understanding and practising online privacy, you can maintain greater control over your digital identity and protect yourself from online threats like identity theft, scams, or unauthorized surveillance.
- **Digital footprint:** Your digital footprint is the trail of information you leave behind while using digital devices and the internet. It encompasses your online activities, including the websites you visit, the social media posts you make, the comments you leave, and the images or videos you share. Your digital footprint can have long-term consequences and can be used by others to track your online behaviour, influence decisions, or even determine your credibility. Understanding your digital footprint is essential to maintain a positive online reputation and protect your privacy.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Some Useful resources

- https://www.digitaleseniorinnen.at/leistungen/know-how
- https://erwachsenenbildung.at/digiprof/mediathek/17725-studie-zu-bildung-und-digitalen-kompetenzen-im-alter.php
- https://cyberclever.eu/resources

A short animation about online navigation and privacy:

- https://www.youtube.com/watch?v=zsboDBMq6vo&list=PL3cjO_EtKN4joc4Gt2lFzBMoZp4h5ty7o&t=51s

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Activity 1#: How to keep and use passwords safely?

Learning objectives:

- Clarify/repeat the purpose of a password
- Learn how to find secure passwords for oneself without write it down
- The rules for “how can you keep your password safe?”

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Settings/materials/duration

- Notes, pens and markers for the participants
- online whiteboard/poster templates (e.g. https://canva.com and/or bigger paper for posters for the participants
- 2 hours

Implementation of the activity:

Step 1 – Introduction:

As an introduction to this activity, ask your participants to make a list of the areas of daily life/websites where they use passwords. It can be written on an online surface (e.g. shared document/whiteboad/worksheet/chat).

Afterwards, you can discuss in plenary how the participants found out about the passwords and whether they had difficulties remembering them or ask this on an online furface as a reflective question.

Step 2:

Ask the participants to research the recommendations on the internet in connection with good passwords.

They can write the rules in a shared document or on a worksheet (in this case ask them to send it to you) and you as a trainer can provide

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

later a poster with the most important rules, which can be shared as a result of the participants work. Participants can print this rules and keep it for guidance in the future.

Support the work with your ongoing feedback on the most important knowledge elements. (See Annex)

Step 3:

Give participants simple methods (see below) on how to generate and notice strong passwords. Present the examples with their own data from a fictitious person. (e.g.: Maria, 76 years old woman, living in a retirement home in Vienna at house number 42, 4 grandchildren, a cat, favourite food is Wiener Schnitzel, favourite colour is light blue) Reflective questions

Example 1: MSchnitzelH42

- Think of your favourite food or vegetable (or a special word.)
- Swap the first letter of it for the first letter of your first name.
- Change the last letter to the first letter of your last name. Add your age, or house number at the beginning or the end.
- Example: ‘Maria Huber’ whose favourite food is ‘Schnitzel’ and she lives at number ‘42’.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Example 2: 3!BabbiT@60

- Try a word that your child/your grandchild couldn’t say properly as a toddler e.g. ‘babbit’ instead of ‘rabbit.’
- Add the number how old he/she was, e.g. 3 and exclamation mark ‘!’ --> 3!babbit
- Make the first ‘b’ a capital ‘B’ and the last ‘t’ a capital ‘T’ --> 3!BabbiT
- Then add @60 at the end because you were 60 at the time. --> 3!BabbiT@60

Example 3: Pntbcaloe2M

- The first letter method: **P**assword **n**eeds **t**o **b**e **c**hanged **a**t **l**east **o**nce **e**very **2** **M**onths --> Pntbcaloe2M
- For this example, you can use a phrase/quotation/line from a poem, etc. that you will probably never forget in your life.

Step 4

Discuss with participants in an online session what they should do if their password is used by someone else or stolen. Mainly password abuse needs to be reported at once to the coordinator of the website, where the password has been stolen.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Research with the participants or encourage them to make a research how these cases are dealt with in their country. There are countries that have a Centre for Internet Security, for instance, where these problems can be reported.

Recommendations for implementation

- It may be that your participants have previously used different rules for dealing with passwords. (E.g. they stored passwords in their mobile phone/wrote them down in a notebook and kept them on their desk, or in Google Drive in a document called “passwords and usernames”). They need more patience and time to work through that maybe they should change their practices.
- Encourage to spend enough time practising a method that your participants can use with confidence. You can ask them one by one if they could find a good functioning method.
- You can set a reminder in mobile phones or in the calendar together every 2 months to change the most important passwords.

Reflective questions

- Have you found a method that helps you make strong passwords?
- What is the best way to notice your passwords?
- Will you do your password management differently in the future? How?

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Activity 2#: Keep personal information safe – stories about privacy

Learning objectives:

- To know the different forms of cybercrime
- Recognise the most important rules in the context of privacy security.
- To know the difference between secured and unsecured networks
- To know how to protect your privacy in open spaces
- To be mindful of online activities and achieve a more safer online experience

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Settings/materials/duration

- Notes and pens for the participants
- online whiteboard
- 1,5-2 hours

Implementation of the activity:

Step 1 – Introduction

This activity is meant either for beginners who do not have much information about privacy, or for older people who may already have had problems with these situations. The activity is also suitable to identify common rules for a community of older people.

Step 2

In case of a self-paced session ask the participants to read the 3 stories.

In the case of an online group session, organize the participants into 3 groups. Give the single groups 1-1 case descriptions (see Annex). The groups should discuss the stories thoroughly, answer the questions related to them. In the case of working individually, the questions are the same.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Especially important is how the victims can avoid the unwanted incident next time.

Step 3

Have the participants present the scenarios and their elaborated answers in an online plenum or on an online surface. If you work with a group, give the participants of the other groups the opportunity to add to the answers if they find it useful. In the case of self-paced learning, provide feedback for your participants.

Step 4

Ask the participants to summarise the most important behavioural rules in at least 5 points based on the scenarios, which can help to avoid such unwelcome stories. It can be shared as usual in this module.

- Recommendations for implementation
- If you know the circumstances of your participants, you can rewrite the stories accordingly.
- If your participants/group live together or meet regularly and have a social worker e.g. in a retirement home/club for elderly people, try to consult with colleagues to rewrite the scenarios according to their needs.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Reflective questions

- Did you learn anything useful from these stories? Could you summarise it briefly?
- Are there any rules that you like to tell your friends or acquaintances?
- Which rule is most important for you?

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Activity 3#: Online banking without fear

Learning objectives:

- Realise the benefits of online banking.
- To recognise the possibilities of online banking.
- To understand the importance of the main rules of online banking in order to be an informed user.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Settings/materials/duration

- computers or personal devices (smart phone, tablets, laptops, etc.) with internet access
- marker, notes, pens for the participants
- Min. 2 hours

Implementation of the activity:

Step 1 – Introduction

Elderly people are often afraid of online banking, since this approach seems to be too unsafe for them. So our goal is in the first step to testify and get closer to their fears so that we can understand under which circumstances we should work.

Explain the aim and the learning objectives of this activity, and pay attention to the recommendations.

Step 2

Ask your participants to form small groups. These small groups should discuss and collect which advantages and disadvantages/risks of online banking they know. It can be written by a participants or on an online whiteboard/table/template, or you can ask them to answer this question individually.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

If you have the opportunity, you can discuss each of these contributions with the group in plenum.

Step 3

Ask all participants to research videos on the internet about online banking. The information collected can be added to the list that had been created in step 2.

Step 4

Encourage you participant to select a few banking institutions whose online system they would like to become familiar with. Of course, you can choose the online banking option of their individual bank which they have known well for a long time. Research of online tutorial videos is recommended. According to the knowledge level they can make it for themselves or you can provide them.

Step 5

Make a summary of the safety rule (for some example see Annex).

Highlight what can and cannot be required from banking institutions or, in the case of online shopping, from users.

Produce this rule in an appealing way and distribute it in the group. (e.g. edit a common poster and provide it as a trainer and share with the participants online)

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Step 6

Discuss the reflective questions with the participants.

Recommendations for implementation

- The aim of this activity is primarily not to convince the participants to choose online banking, but to give information to overcome their fears of this technique, to show new perspective and to empower open persons to use online banking after having prepared thoroughly.
- If you have the opportunity, you can hold follow-up seminars where participants who tried out online banking can share their first experiences.

Reflective questions

- Do you feel more secure when you think about online banking now?
- Is online banking clearer for you now?
- What do you think, could you do your banking online now with more confidence?
- If you feel like trying online banking, who can you ask for help/ support from?

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Evaluation of the Module

Quiz for Self-Assessment for Module 9

To be answered by learners at the end of the module to measure the extent to which the training objectives were achieved.

https://forms.gle/kHphuJEzTt98SwpL8

Worksheet

Key questions are formulated and learners set out hypotheses, design procedures to test their hypotheses, and present their findings. Their answers provide the basis for discussion and identification of possible misconceptions, or gaps in understanding.

https://forms.gle/ouLnaxijfTLS8WzL7

Project-Activity

Learners are able to solve a practical task with the creative, independent and result-oriented application of the acquired knowledge, skills and competencies.

Project tasks could be solved in small groups (if the modules are completed in a training course)/ or individual.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

You can find suggestions here, specific project tasks should be customised to the needs and to the starting knowledge level of the target group and to the goals to be achieved.

- Make short showcase videos about privacy issues (similarly to the elaborated descriptions on the course) in open spaces. Participants' opinions/knowledge transfer can also be added at the end of the films. These videos can also be used later as teaching materials.
- Organise with the participants some community of practice events in the community of older people. Your participants, with your support, can give shorter presentations to their peers about password-managing or online banking and share some practical lessons they have already acquired.
- Social media page for older people - support the creation of a social media page for older people, where short posts about the most important privacy issues are regularly shared. Participants can first make a list of topics: the more specific the better. The processed topics can of course be used here very well, so that the participants can experience that they have not only implemented the various activities for themselves and in vain.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Questionnaire

To be answered by learners at the end of the module to measure the overall impact of the training program. These can be compiled also in the form of test questions with multiple possible answers.

https://forms.gle/dNLiYiZTz4eMqCqq6

Validation of the Module

At the end of the Module, learners will have acquired

Knowledge:

The learners are able to

- understand the meaning of personal data and privacy,
- identify the different forms of cybercrime,
- consciously manage their individual settings in various platforms,
- know exactly what minimum conditions are needed to rate a website secured,
- apply a solid knowledge of when managing passwords and online banking apps.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Skills:

The learners are able to

- use consciously strong passwords
- recognise the cases when someone's privacy is breached.
- report to the appropriate organisations if they notice their passwords or data have been mishandled.
- control their own online activities in a self-responsible way.

Competencies:

The learners are able to

- handle own passwords and personal data's with self-responsibility in the online world,
- support and defend the privacy of oneself,
- respect the privacy of other users,
- use the advantages of the online apps and websites without fear but carefully and consciously.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

ANNEX For Module 9

Media Literacy & Privacy

Entry Level Test - Media Literacy & Privacy

Question 1: It is safe to use the same password for multiple online accounts.

a. True
b. False

Question 2: Which of the following is a recommended practice for protecting personal information online?

a. Sharing personal information on social media platforms.
b. Keeping personal information saved on public computers.
c. Regularly updating privacy settings on social media accounts.
d. Clicking on unknown email attachments.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Question 3: Online banking is not safe for elderly people.

a. True
b. False

Question 4: Privacy settings allow individuals to control who can access their personal information on social media platforms.

a. True
b. False

Correct answers:

Question 1: b) False

Question 2: c) Regularly updating privacy settings on social media accounts.

Question 3: b) False

Question 4: a) True

Exit Level Test - Media Literacy & Privacy

Question 1: Privacy settings and permissions, such as cookies, have no impact on protecting personal information online.

a. True
b. False

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Question 2: Which of the following is NOT a basic rule for ensuring online privacy and personal information protection?

a. Avoid sharing personal information on social media platforms
b. Use strong and unique passwords for different online accounts
c. Click on suspicious links or download files from unknown sources
d. Keep software and antivirus programs updated

Question 3: Online banking is a safe and secure option for elderly people, and they should feel confident in using it.

a. True
b. False

Question 4: Which of the following actions can help keep personal data safe?

a. Using the same password for multiple online accounts.
b. Sharing personal information on social media platforms.
c. Opening email attachments or clicking on suspicious links.
d. Regularly updating passwords and using strong, unique passwords for each online account.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Correct answers:

Question 1: b) False

Question 2: c) Click on suspicious links or download files from unknown sources

Question 3: a) True

Question 4: c) Regularly updating passwords and using strong, unique passwords for each online account.

Activity 1#: How to keep and use passwords safely?

Step 2

Links for safety password:

- https://edu.gcfglobal.org/en/internetsafety/creating-strong-passwords/1/
- https://www.webroot.com/us/en/resources/tips-articles/how-do-i-create-a-strong-password
- https://terranovasecurity.com/how-to-create-a-strong-password-in-7-easy-steps/
- https://www.rhsb.com/your-passwords-hackable/

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Activity 2#: Keep personal information safe – stories about privacy

Scenario 1:

Bill meets with his old friends and colleagues in a café twice a week. In the meantime, he wanted to discuss something with other people on the social media sites. He logged in with his simple password and by now he was saying a few letters out loud to make sure he was doing everything well. His friends also looked at his mobile phone. Later, he went to the toilet and left his mobile phone on the table because he didn't want to take it with him so that it wouldn't get wet. When he returned, his friends were busy chatting on his mobile phone. What could happen next?

Possible answers:

- If the friends on the chat have not mentioned that they are not identical to the owner of the mobile phone, this can lead to unpleasant misunderstandings.
- Mean messages could also be sent.
- Important connections can be cancelled or unwanted ones can be made.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Important data may be stored on an unlocked mobile phone, which could be used by malicious misusers for unwanted purposes.

Recommendations:

- Never leave your mobile phone unattended.
- Use a strong password
- Never speak your data out loud in public places.

Scenario 2:

Sylvia was using her laptop in the community room. Georg had some visitors, but she did not know them. Sylvia logged on her laptop, because she was talking to her friends online and wanted to share some photos from her holiday with her grandchildren. Daniel and Michael, the visitors were watching her on her laptop all the time. After an hour, Sylvia wanted to drink a glass of water and went to the kitchen. She left her laptop on the table. She had a few words with the others in the kitchen and was back in 10 minutes. In the evening she had already received 6 messages from her friends about what was wrong with her, sending such nasty messages after a pleasant afternoon chat. What could happen?

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Possible answers:

- the visitors don't know and adore the rules of the community, so they probably sent messages for Sylvia's friends.
- Sylvia has probably not unsubscribed from the chat.
- She probably does not have a password to enter on her laptop or it is too weak.

Recommendations:

- Never leave your personal devices unattended
- Use a strong password
- Publish the rules of the community in open spaces

Scenario 3

Dorothea had gone with her friend to a pleasant restaurant with a garden for lunch. There were just a few seats, so two men asked them to sit at the other end of the long table. They wanted to joke with Dorothea and her friend, but they only wanted to talk to each other. After 15 minutes they had the opportunity to sit at another small table and leave the men behind them. But a little later Dorothea noticed that she had left her bag with her mobile phone on the other table. She didn't have a complicated code (1234) and her online bank was open because she checked that she had enough money in her account just before lunch. What could happen next?

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

Possible answers:

- Unfortunately in this case all the login details may be stolen, and in the worst case scenario Sylvia's bank details may be used to transfer her money and account in full to another account or to pay small or large sums regularly from here. She should change all login details immediately, possibly banning the use of the account for a short time.

Recommendations:

- Never leave your personal devices unattended
- Use a strong password
- If you are not sure to always supervise your tools, do not use sensitive apps in open spaces (e.g. online banking and other important online services) and log out when you have finished using them. In this case, never store passwords in your personal device.

Activity 3#: Online banking without fear

Step 5:

What can I do to keep my money and identity safe?

Generally, online banking is safe, but there are steps you can take to look after your money and identity:

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

- **Use a strong password** that avoids common words, numbers or keyboard patterns (such as ‘password’ or ‘123456’). Don’t include personal information, such as your name, date of birth, or any family member’s details in your password. Click here to find out more about how to choose a strong password.
- **Don’t reuse passwords for different accounts.**
- **Never share your full password or PIN number.** Banks will never ask for your full PIN or password – instead, they’ll ask for specific numbers or letters, for example, the first and third character.
- **Always log out of your online banking session,** especially if you’re using a shared device. If you’re using a public computer, like a library computer, be particularly cautious – they may not have the right level of security software. If you need to, ask the library staff for more information.
- **Only use secure Wi-Fi networks to access your online banking.** If you use a public network, such as those in cafes or train stations, it may be possible for people on the same network to access your details.

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

- **Check your balance and transactions regularly.** If there's a transaction you don't recognise, report it to your bank straight away.
- **Regularly check that your personal details are correct and up to date.**

Resource:

Online banking for older people | Age UK

MEDIA LITERACY & PRIVACY QUIZ

! This quiz is part of the Information Matters Training Programme (co-funded by the Erasmus+ Programme of the European Union), Module 9 - Media Literacy & Privacy for Older People. (Please choose the right answer.) (Info for trainers: right answers are marked with x, do not forget to adapt the quiz for your target group.)

- **My password**
  a. have to be created by me. (x)
  b. is created for me by my social workers/doctors/relatives/nurse

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

» A password

a. can never be changed in my life.
b. have to be changed regularly. (x)

» It is recommended to change important passwords

c. at least every 2 months. (x)
d. at least yearly.
e. at least every 2 years.

» A strong password should contain

a. small letters (x)
b. capital letters(x)
c. only capital letters
d. special characters (x)
e. only special characters
f. numbers (x)
g. min. 8 characters (x)
h. max. 8 characters
i. personal datas
j. my mothers name

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

» I should always

a. keep my password close to my computer or other devices.
b. keep passwords secret. (x)
c. share my password with my social worker/nurse/relatives/ friends.

» When I use my mobile devices in open spaces,

a. I have to give it to my friend to watch it when I have something else to do.
b. I should never leave it unlocked so that no one has access to my data. (x)
c. I am safer than at home.

» If I want to arrange something in my bank,

a. the bank will neer ask for my full PIN or password. (x)
b. the bank will ask for my full PIN and password.

» It is okay, to access online banking

a. on a safe privat computer at home. (x)
b. on public networks, like in cafes or train stations.

» It is okay

a. to use the same password for my accounts.
b. to always use different passwords for my accounts. (x)

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

MEDIA LITERACY & PRIVACY Questionnaire

! This questionnaire is part of the Information Matters Training Programme (co-funded by the Erasmus+ Programme of the European Union), Module 9 - Media Literacy and Privacy for Older People.

Information Matters – Information Matters

» **Did the training content about media literacy & privacy meet your expectations?**

a. Yes
b. No

» **Was the mix of presentations/explanations and activities suitable?**

a. Yes
b. No

» **Did you learn anything new?**

a. Yes
b. No

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

If yes, please provide more details about your acquainted knowledge skills/competencies. I am able to...

If no, please provide details about missing knowledge/skills/competencies:

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

» **Was the course practical or easy to apply?**

a. Yes
b. No

» **Have you observed any positive impacts of this course on your privacy issues? Could you specify them?**

» **Based on this training, would you be interested in having trained in other skills?**

a. Yes
b. No

» **Do you have any suggestions to improve this course?**

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

If yes/no, please provide more details, why?

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by the European Union

information matters

contact@informationmatters.eu

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.

Agreement number: 2022-1-BG01-KA220-ADU-000085514

Co-funded by
the European Union