SECURITY
IN THE DIGITAL WORLD

Training program with workshop scenarios and materials for educators on cyber security of seniors

TABLE OF CONTENTS

1. Introduction

The “Cyber Safe Senior” is a European Union-funded project aimed at improving digital literacy, online safety, and general digital empowerment among seniors aged 65 and up. In today's increasingly digital world, seniors confront special obstacles while navigating online environments since they are often unfamiliar with emerging technologies, online risks, and safe digital behaviors. Recognizing this, the Cyber Safe Senior initiative aims to close crucial gaps in digital knowledge and competence using an organized, accessible, and multifaceted approach.

The project entails creating an informative e-book that includes real-life internet crime case studies, practical safety advice, and step-by-step directions for safe online behavior. In addition, the initiative offers virtual lectures, interactive scenario-based exercises, and pilot training sessions that are specially tailored to the learning goals and preferences of senior participants. Cyber Safe Senior aims to eliminate digital exclusion, improve confidence in technology use, and enable older persons to participate independently and safely in digital environments by concentrating on seniors who have some basic digital experience but lack awareness of online security.

The project's training program for educators and trainers provides them with the information, methodology, and practical tools they need to give high-quality internet safety education to seniors. Trainers are prepared not just to teach essential cybersecurity ideas, but also to engage students in interactive activities, real-life scenarios, and exercises that highlight the unique issues that older persons may experience in the digital world. This guarantees that the training is both practical and directly relevant to the participants' daily life.

The project is being carried out by a consortium of partners from Poland, Slovenia, Turkey, and Greece, who bring together knowledge from educational institutions, community organizations, libraries, cultural centers, and senior citizen communities. Using these local networks, Cyber Safe Senior can reach seniors in both urban and rural locations, ensuring fair access to digital literacy materials and support.

By educating seniors to use online platforms with confidence, safeguard their personal data, identify online risks, and actively engage in digital society, the project aims to create a more secure and welcoming digital environment. In the end, Cyber Safe Senior combines instructional materials, hands-on activities, and community involvement to establish a setting where senior citizens have the information, abilities, and self-assurance they need to use digital tools securely, independently, and productively.

A key complementary component of the Cyber Safe Senior training programme is the set of interactive Improve Case studies developed using Genially. These scenario-based cases are fully aligned with the topics of each training module and are designed to simulate real-life digital situations commonly faced by seniors. Through guided decision-making, practical tasks, and visual interaction, the Improve Cases reinforce theoretical knowledge and support experiential learning, making complex online safety concepts more accessible and engaging for older learners.

Each training module follows a structured format consistent with the module interface, including learning objectives, session planning, additional resources, trainer self-reflection, and evaluation elements. Pre- and post-tests are implemented at the beginning and end of each module to measure knowledge acquisition and learning progress. In addition, evaluation surveys are used to collect feedback from participants and trainers, supporting quality assurance and the continuous improvement of the training programme.

1.1 Aim of the Training Program

The Cyber Safe Senior Training Program is developed to meet the growing need for digital literacy and internet safety among senior adults aged 65 and above. Seniors have difficulties navigating online settings in today's digital world because they usually have little knowledge of possible threats, online security measures, and safe digital habits. The goal of this training program is to close these gaps by giving seniors the tools they need to use digital technologies securely and confidently in an effective, hands-on, and interesting learning environment.

Its objectives are to increase seniors' knowledge of internet safety, provide them with necessary skills, and encourage their confidence in using digital technologies safely. In addition to practical measures to protect personal data and privacy, the training program offers clear awareness of prevalent online threats and how to recognize them, advice on safe online behaviors, and insights into real-life scenarios that illustrate possible threats and remedies. With five extensive courses that run four hours each and ten interactive IMPROVE cases that simulate ad hoc reactions to online threats, the program places a strong emphasis on hands-on learning by examining real-world examples of cybersecurity dangers. Content, thorough exercises with instructions, and the tools and resources required to provide this training program are all included in each session.

These resources give teachers useful activities, supplies, and methods for getting seniors interested in and involved in interactive learning. Teachers who successfully complete this program will be equipped to help elders develop their digital empowerment and confidence.

1.2.1 Key Objectives of the Program

Raise Seniors' Awareness of Online Threats
They will acquire a comprehensive grasp of the most prevalent online threats, such as malware, phishing, frauds, identity theft, and dangerous websites. The program teaches participants how to recognize warning signs and illustrates possible hazards using real-world examples.

Develop Practical Digital Skills
Participants will gain a comprehensive understanding of how to properly carry out typical internet tasks like social media use, online banking, shopping, and browsing. Safe data management, two-factor authentication, and strong passwords are emphasized.

Promote Safe Online Behavior
The program emphasizes the adoption of best practices for privacy protection, safe communication, and ethical digital engagement. Seniors will understand how to manage personal information, recognize fraudulent messages, and respond appropriately to suspicious activities.

Equip Trainers with Expertise
Training educators and facilitators is a fundamental part of the program. Trainers will gain the skills, resources, and techniques required to provide senior-focused, online safety instruction. This covers advice on managing group dynamics, scenario-based learning, and interactive teaching techniques.

Reduce Digital Exclusion
The program aims to reduce seniors' social and technological isolation, especially for those who live outside of urban areas, by enhancing digital literacy and knowledge of online safety. In today's digital world, participants will get more comfortable utilizing digital devices on their own, promoting more inclusivity.

1.2.2 Expected Outcomes

- Seniors will get the knowledge and practical skills necessary to safely navigate internet environments.
- Trainers will be well-equipped to provide senior citizens with interesting and useful cybersecurity instruction.
- Seniors with digital empowerment who can engage in online activities and services in a safe manner will benefit their communities.

The training program combines theory with interactive, scenario-based exercises, case studies, and group activities to ensure that learners learn through doing. Each module contains structured information, practical tasks, and discussion opportunities, allowing seniors to use their knowledge instantly and acquire confidence in real-world situations. The program also incorporates evaluation and reflection components, which ensure that learning outcomes are met while also offering feedback for both trainers and participants to develop themselves continuously.

1.2.3 Improve Cases

The IMPROVE Cases are interactive, scenario-based learning activities intended to supplement the Cyber Safe Senior training modules. These scenarios are directly related to Modules I-V and demonstrate true online situations that seniors may meet in their daily digital interactions, such as phishing emails, online shopping fraud, dangerous public Wi-Fi use, and fraudulent investment scams. The scenarios, delivered via interactive Genially content, allow participants to identify possible threats, make informed decisions, and comprehend the effects of risky online activity. The IMPROVE cases encourage hands-on learning by replicating real-life digital threats, allowing seniors to build practical skills for safer internet use.

The Improve Cases are aligned with the training modules according to their thematic focus and learning objectives.

- **Module I – Cybersecurity Basics: Protecting Your Computer, Email, and Personal Data:** Smishing; The Public Wi-Fi Dilemma.
- **Module II – Common Online Scams Targeting Seniors:** Grandparent Scam; The Charity Fraud Trap.
- **Module III – Online Banking and Shopping Safety:** Online Shopping Scams; E-mail Phishing Scam; Crypto Mirage: The Illusion of Instant Wealth; Golden Returns – The Price of Trust.
- **Module IV – Safe and Responsible Social Media Use for Seniors:** Deepfake Scam; Online Service Type Scam.
- **Module V – Safe Digitalization of Seniors:** Covered transversally through the overall training content and activities.

Access to Improvement Cases:

- Crypto Mirage: The Illusion of Instant Wealth
- Online shopping scams
- The charity fraud trap
- Smishing
- The public Wi-Fi dilemma
- E-mail phishing scam
- Grandparent scam
- Online service type scam
- Deepfake scam
- Golden Returns – The Price of Trust: An Investment Fraud Case

MODULE I

Cybersecurity basics protecting your computers, email, and personal data

2. Module I - Cybersecurity basics protecting your computers, email, and personal data

The “Cybersecurity Basics" module offers a complete overview of digital security, integrating theoretical knowledge with practical applications. Participants will receive a thorough understanding of the essential principles of computer security, email privacy, and personal data protection. The module covers important sub-topics such computer security and email management, in which students will learn how to maintain their operating system and software, utilise antivirus programmes and firewalls, and identify potential cyber threats. It also focuses on password security and administration, teaching users how to establish strong passwords and use password managers successfully.

Practical email security exercises are provided, teaching participants how to recognise phishing attempts, identify suspicious links or files, and monitor their mailboxes for unauthorised activity, including the use of two-factor authentication for enhanced security. The programme also discusses how to secure personal devices such as computers, cellphones, and tablets, including tactics for screen locking, monitoring lost devices, avoiding unauthorised physical access, and keeping software up to date to protect against developing threats. Finally, the programme focuses on personal data management and online privacy, teaching students how to alter privacy settings on social media, protect critical information, and safely utilise public Wi-Fi networks using VPNs.

By combining these sub-topics, the training ensures that seniors not only comprehend potential threats in digital surroundings, but also learn practical methods to defend themselves. Participants will leave the module with more awareness, confidence in dealing with cybersecurity concerns, and the capacity to implement acquired solutions in real-world scenarios.

2.1 Learning Objectives

The main objective of this module is to equip participants with practical knowledge and skills necessary for effectively protecting computers, email accounts, and personal data from threats in cyberspace. Participants will learn how to identify potential threats, minimize risks, and implement strategies to enhance digital security in both their personal and professional lives.

- Understand the fundamental principles of cybersecurity that help prevent attacks and protect data from unauthorized access.
- Develop skills to create strong passwords and store them securely, increasing resilience against breaches.
- Recognize and avoid phishing attacks, which are one of the most common methods of online fraud.
- Effectively secure personal devices and the data stored on them by using tools such as encryption, screen locks, and location tracking features.
- Manage privacy settings on social media platforms consciously to reduce the risk of personal data leaks.
- Gain knowledge and skills for safely using public Wi-Fi networks by employing VPNs and other protective tools.

2.2 Structure, Content & Learning Outcomes

On successful completion of this module, learners will be able to:

- **Introduction to basic computer security:** how to update the operating system and software, use antivirus programs and firewalls, how to identify signs of potential attacks on the computer and how to minimize the risk of their occurrence.
- **Creating secure passwords and storing them:** how to create strong passwords consisting of unique combinations of letters, numbers and symbols, how to use password managers to avoid storing passwords in an unsafe way, e.g. on paper.
- **Practical scenarios for detecting email phishing:** analyze sample phishing messages and learn how to recognize suspicious links, attachments or language errors, how to report suspicious e-mails to the appropriate services.
- **Monitoring and securing your mailbox from unauthorized access:** how to set up two-step verification, monitor unusual activity in your mailbox, and respond to hacking attempts.
- **Protecting personal devices (computers, smartphones, tablets):** how to lock the screen and use applications that allow you to locate lost devices, how to protect your devices from physical access by unauthorized persons.
- **Protecting personal devices (computers, smartphones, tablets):** how to lock the screen and use applications that allow you to locate lost devices, how to protect your devices from physical access by unauthorized persons.
- **Regular software updates for increased security:** why regular updates are necessary to protect your devices from new threats, and how to configure the system for automatic updates.
- **Protecting your privacy on social media:** How to adjust privacy settings on popular social media platforms, what information should be kept private, and how to avoid sharing data that could be used in an undesirable way.
- **Rules for safely using public Wi-Fi networks:** risks of using open Wi-Fi networks and how to use a VPN to protect your data when connecting to the internet in public places.

2.3 Agenda | Detailed Session Plan

MODULE I
Cybersecurity basics | Protecting your computers, email, and personal data

1st Session

Welcome
Duration *5 min*

Learning Objectives

- Creating an open and engaging atmosphere conducive to active participation.

Content/ Method

- Welcoming the participants and a brief introduction of the trainer.
- Presenting the training agenda and working rules.

- Encouraging participants to introduce themselves (name and one word associated with cyber threats).

Material
No additional materials.

Comments
It may be helpful to present the purpose of the workshop in simple language.

2nd Session

Icebreaker Activity: "Cybersecurity Basics"
Duration *15 min*

Learning Objectives
- Learning and understanding basic cybersecurity terms.
- Reinforcing knowledge of cybersecurity.

Content/ Method
- Carrying out an exercise involving matching concepts to definitions.
- Participants receive a worksheet (Appendix 1). The task of the participants is to correctly match each concept to its corresponding definition. The exercise is individual or team-based, depending on the decision of the leader. After completing the task, the trainer moderates a short discussion during which the answers are discussed, any ambiguities are clarified, and issues related to the subject of the exercise are explored. Encouraging participants to introduce themselves (name and one word associated with cyber threats).

Material
- Worksheet, Icebreaker: "Cybersecurity Basics" (Appendix 1)

Comments
This task introduces the topic and allows you to assess the participants' initial level of knowledge.

3rd Session

Lecture 1: Computer security and email
Duration *20 min*

Learning Objectives
- Understand the importance of keeping your system and software up to date.
- Recognize the different types of cyber threats, including malware, spyware, and ransomware.
- Understand the role of antivirus software in keeping you safe.
- Gain the knowledge and skills to safely use public Wi-Fi networks by using VPNs and other security tools

Content/ Method

- A lecture explaining the basic concepts: why regular system updates are crucial, how malware penetrates systems and what the role of antivirus software is and how to recognize a secure Wi-Fi network.
- Using real-life examples (e.g. known ransomware attacks) to illustrate the risks associated with outdated systems and unsecured devices.
- Highlighting best practices such as enabling automatic updates and avoiding suspicious downloads. To implement the lecture, the trainer has at their disposal the topic suggestions provided in Appendix 2.

Material

- Proposal of topics to be discussed (Appendix 2)

Comments

It is worth encouraging participants to actively participate in the lecture by allowing them to ask questions.

Activity 1 "Quiz: True/False"
Duration *20 min*

Learning Objectives

- Consolidation of knowledge from the lecture, development of awareness of threats.

Content/ Method

- The course includes an exercise in the form of a quiz called "True or False?", conducted on the basis of a worksheet (Appendix 3) that participants receive from the instructor.
- Participants have 5 minutes to mark their answers independently. After completing this stage, the trainer moderates a short discussion during which the correct answers are discussed with the group, important issues are explained, and any misconceptions are corrected. Finally, the trainer summarizes the key content covered in the quiz, reinforcing understanding and consolidating good practices related to digital security.

Material

- Worksheet Quiz: True/False (Appendix 3)

Comments

Summarize key points after the quiz to reinforce participants' understanding of essential security practices.

Break | Duration *5'*

- **Allow time for participants to recharge and reflect.**
- **Short break to refresh.**
- **Encourage participants to stretch or grab a drink to recharge before the next lecture.**

4th Session

Lecture 2: Practical exercises related to email security
Duration *30 min*

Learning Objectives

- Learn best practices for creating strong, secure passwords (e.g., using upper- and lowercase letters, special characters, and numbers).
- Understand the risks of poor password storage and learn about password managers.

Content/ Method

- Explain the "three-component rule" (length, complexity, uniqueness) for creating strong passwords. Demonstrate how password managers work and discuss their benefits (e.g., increased security, convenience). Highlight common mistakes, such as reusing passwords or storing them in unsecured files.

Material

- Proposal of topics to be discussed (Appendix 4)

Comments

Provide relatable, practical tips, such as creating a password based on an easy-to-remember but unique phrase.

Activity 2: Creating strong passwords
Duration *20 min*

Learning Objectives

- Practice creating strong, unique passwords following the guidelines discussed.

Content/ Method

- The exercise is carried out in two stages – first individually, then in pairs. A worksheet (Appendix 5) has been prepared for the exercise.
- Participants independently create at least three strong passwords in accordance with security principles, writing them down on cards. Then they show them to their partner from the pair, who assesses their length, complexity and uniqueness, providing feedback and possible suggestions for improvement. At the end, the trainer discusses the features of a secure password and initiates a discussion with the whole group, enabling the exchange of reflections and good practices.

Material

- Worksheet Creating Strong Passwords (Appendix 5)

Comments

It is worth encouraging participants to pay attention to whether the passwords they currently use are secure according to the instructor's instructions.

Break | Duration *5 min*

- **Provide time to rest and prepare.**
- **Short break to refresh.**
- **Short break for refreshment and relaxation.**

5th Session

Lecture 3: Securing personal devices and information
Duration *30 min*

Learning Objectives

- Gain knowledge on how to recognize phishing emails.
- Understand how to configure basic email security settings.

Content/ Method

- Explains the telltale signs of phishing, such as misspellings, unknown sender addresses, and urgent messages. Shows how to adjust email security settings on platforms like Gmail and Outlook. Shows examples of phishing emails and discusses how to recognize the red flags.

Material

No additional materials needed.

Comments

Showing real cases of phishing from popular services (e.g. PayPal, Amazon) in order to make the content more attractive

Activity 3: Analyzing phishing e-mails
Duration *20 min*

Learning Objectives

- Practical email analysis – detecting irregularities.

Content/ Method

- The trainer has a set of email templates at their disposal (Appendix 6), which should be enriched with details before being distributed to participants – such as sample links, names of well-known companies (e.g. banks, courier services or shopping platforms).
- The exercise is carried out in pairs or small groups. Participants analyze prepared emails from the worksheet (Appendix 6), identifying and marking suspicious elements. After the analysis is completed, there is a joint discussion moderated by the leader.

Suggested questions for discussion:

- What warning signals are found in this email?
- How can you protect yourself from such an attack?
- What should you do if you receive a suspicious email of this type?
- Prepare to discuss the answers with the group.

Material

- Worksheet, Phishing Email Analysis (Appendix 6)

Comments

Summary of group analysis results, highlighting key differences between real and fake emails.

Break

Duration 5 min

- **Provide time to rest and prepare.**
- **Short break to refresh.**
- **Short break for refreshment and relaxation.**

6th Session

Lecture 4: Managing personal data and online privacy

Duration *30 min*

Learning Objectives

- Communicating privacy policies, privacy settings, locks, and updating. Communicating basic security settings to protect devices (e.g., enabling screen locks and automatic updates).
- Understanding how to effectively manage online privacy settings.

Content/ Method

- Discuss ways to protect your data on social media (Instagram, Facebook), privacy settings on smartphones, and app sharing restrictions.
- The trainer discusses key security settings on smartphones and computers, such as screen locks, data encryption, app management, and permission settings on Android and iOS.
- Discuss online privacy management – how to set privacy settings on social media platforms, controlling who can see posts, personal information, and which apps have access to your data.
- Discuss the principles of checking Wi-Fi security – how to recognize unsecured connections, why you should avoid unprotected public networks, and how to increase the security of your home internet network.
- Emphasize the importance of regularly reviewing privacy settings – the importance of periodically reviewing and updating privacy settings to adapt to changing needs and new online threats.

Material

No additional materials needed.

Comments

Focus on practical, easy-to-implement steps to enhance device security and privacy.

Activity 4: Secure device configuration
Duration *20 min*

Learning Objectives

- Applying knowledge by configuring security settings on personal devices.

Content/ Method

- Participants practice setting up a screen lock, enabling two-step verification, and adjusting privacy settings. The trainer provides individual support as needed.

Material

- Smartphones and/or computers.

Comments

Encourage participants to troubleshoot and ask questions as they configure their devices.

7th Session

Discussion
Duration *10 min*

Learning Objectives

- Reflect on the key lessons learned.
- Encourage participants to share their most valuable takeaways and remaining questions.

Content/ Method

- A moderated discussion in which participants share their observations, experiences and questions that require clarification. The trainer summarizes key points and addresses questions.

Material

No additional materials needed.

Comments

Encourage participants to connect the learned concepts to their everyday online behavior.

Wrap Up
Duration *5 min*

Learning Objectives

- Summarize key learning points and provide resources for further learning.
- Thank participants and close the session.

Content/ Method

- Summary of key learnings from the training.
- Sharing additional resources (e.g. cybersecurity websites, articles).

- ❖ Thanking participants for their engagement and encouraging them to continue improving their cybersecurity practices

Material

- ❖ Recommendations for further reading and learning for participants (Appendix 7)
- ❖ Cybersecurity websites: European and governmental cybersecurity organizations

Comments

Finally, it is worth conducting a short evaluation survey.

2.4 Additional Information

2.4.1 Trainers' Self Reflection

- ➢ Did I clearly and effectively convey to participants the importance of online safety and conscious use of social media?
- ➢ Did I use practical examples that helped to better understand digital threats?
- ➢ Did I ensure that participants understood the technical aspects of privacy settings and scam recognition?
- ➢ Did I ensure that participants understood the technical aspects of privacy settings and were able to recognize scams such as phishing?
- ➢ Did I adapt the information provided to the level of advancement of participants?
- ➢ How did I engage participants during activities and discussions?
- ➢ Did I encourage active participation, sharing experiences and asking questions?
- ➢ Were the materials and resources used (e.g. presentations, quizzes, practical exercises) helpful and appropriate for participants?
- ➢ Were the materials prepared clear and easy to understand?

2.4.2 Trainers' Evaluation of the Program

- ➢ Was the training content relevant to the needs of seniors and appropriately adapted to their level of knowledge and experience?
- ➢ Did participants have the opportunity to understand the basic principles of cybersecurity and online privacy?
- ➢ Did activities such as quizzes, practical exercises, and analysis of phishing examples support the learning process of participants?
- ➢ Did the discussions allow for deepening knowledge and encouraging reflection on digital security?
- ➢ Are the achieved outcomes (e.g. understanding digital threats, ability to configure security settings) in line with the intended educational goals of the module?
- ➢ Did participants master key skills such as creating strong passwords, recognizing fraud, and managing online privacy?

2.4.3 Materials, Additional Resources

Appendix 1 | Worksheet Icebreaker Activity: "Cybersecurity Basics"

Match the concept with the correct definition:

Phishing	**a fraudulent method of impersonating trusted entities to steal sensitive data.**
Ransomware	**malicious software that encrypts data and demands a ransom for its release.steal sensitive data.**
Two-Factor Authentication (2FA)	**an additional security layer requiring a second authentication factor.**
Passwords & Password Managers	**strategies for managing strong and unique passwords for different services.**
Firewall	**a security system that protects against unauthorized access to a network.**
Data Encryption	**a method of protecting data from unauthorized access by converting it into unreadable code.**
VPN (Virtual Private Network)	**a technology that ensures secure and private internet connections.**
Secure Email	**practices for protecting email messages from attacks, such as spam filtering and encryption.**
SOC (Security Operations Centre)	**an operations center responsible for monitoring and responding to cybersecurity threats.**

Appendix 1 | Worksheet Icebreaker Activity: "Cybersecurity Basics"

Correct answers

1. **Phishing** – a fraudulent method of impersonating trusted entities to steal sensitive data.
2. **Ransomware** – malicious software that encrypts data and demands a ransom for its release.
3. **Two-Factor Authentication (2FA)** – an additional security layer requiring a second authentication factor.
4. **Passwords and Password Managers** – strategies for managing strong and unique passwords for different services.
5. **Firewall** – a security system that protects against unauthorized access to a network.
6. **Data Encryption** – a method of protecting data from unauthorized access by converting it into unreadable code.
7. **Malware** – software designed to harm users or computer systems.
8. **VPN (Virtual Private Network)** – a technology that ensures secure and private internet connections.
9. **Secure Email** – practices for protecting email messages from attacks, such as spam filtering and encryption.
10. **SOC (Security Operations Center)** – an operations center responsible for monitoring and responding to cybersecurity threats.

Appendix 2 | Suggested Topics to Discuss Lecture 1 | Computer and Email Security

- The importance of regular updates to operating systems and applications.
- The risks of outdated systems and unsecured devices.
- Types of malware: viruses, Trojan horses, ransomware, and how they work.
- The mechanisms that allow malware to infiltrate systems.
- The role of antivirus software in protecting against cyber threats.
- Using firewalls to protect against attacks.
- Password management practices, including the use of password managers.
- Rules for avoiding dangerous attachments and suspicious links in emails.
- The importance of data encryption in protecting privacy and security.
- Automatic updates as a best practice in ensuring security.
- VPNs and their role in protecting online privacy.
- Why not every free Wi-Fi network is safe?
- Basic email protection against phishing and spam.
- Best practices for creating strong passwords and their impact on security.
- Mobile device and application security.
- The importance of user education and awareness in preventing cyberattacks.

Appendix 3 | Worksheet Quiz: True/False

Mark which statements are true, and which are false.

- Regular updates to the operating system and applications are only necessary for new devices. **True/False**
- Malware, such as viruses or trojans, can infiltrate systems through outdated software and security vulnerabilities. **True/False**
- Antivirus software is unnecessary if the system is regularly updated. **True/False**
- A firewall is only used to protect against physical attacks on devices. **True/False**
- Password management and the use of password managers are crucial in maintaining strong, unique passwords for various services. **True/False**
- Avoiding suspicious attachments in emails is not important if antivirus software is installed. **True/False**
- Data encryption helps protect privacy and security from unauthorized access. **True/False**
- Automatic updates are optional because manually updating the system is always enough to ensure security. **True/False**
- A VPN (Virtual Private Network) allows for a secure connection to the internet, hiding our online activity. **True/False**
- Phishing is an attack technique that involves stealing passwords through seemingly trustworthy emails. **True/False**
- A strong password should only consist of letters and be easy to remember so that it is not difficult to use. Mobile devices require fewer security measures than desktop computers, as they are less prone to attacks. **True/False**
- Mobile devices require fewer security measures than desktop computers, as they are less prone to attacks. **True/False**
- User knowledge about online threats is essential in preventing cyberattacks. **True/False**
- Ransomware is software that blocks access to a system or files and demands a ransom for unlocking them. **True/False**
- An outdated operating system is secure because older versions of software are rarely targeted by attacks. **True/False**

Appendix 3 | Worksheet Quiz: True/False
Correct answers

1. Regular updates to the operating system and applications are only necessary for new devices. - False
2. Malware, such as viruses or trojans, can infiltrate systems through outdated software and security vulnerabilities. - True
3. Antivirus software is unnecessary if the system is regularly updated. - False
4. A firewall is only used to protect against physical attacks on devices. - False
5. Password management and the use of password managers are crucial in maintaining strong, unique passwords for various services. - True
6. Avoiding suspicious attachments in emails is not important if antivirus software is installed. - False
7. Data encryption helps protect privacy and security from unauthorized access. - True
8. Automatic updates are optional because manually updating the system is always enough to ensure security. - False
9. A VPN (Virtual Private Network) allows for a secure connection to the internet, hiding our online activity. - True
10. Phishing is an attack technique that involves stealing passwords through seemingly trustworthy emails. - True
11. A strong password should only consist of letters and be easy to remember so that it is not difficult to use. - False
12. Mobile devices require fewer security measures than desktop computers, as they are less prone to attacks. - False
13. User knowledge about online threats is essential in preventing cyberattacks. - True
14. Ransomware is software that blocks access to a system or files and demands a ransom for unlocking them. - False
15. An outdated operating system is secure because older versions of software are rarely targeted by attacks. - False

Appendix 4 | Suggested Topics for Lecture 2 " Email Security Practical Exercises"

- Creating Secure Passwords – principles for creating strong passwords that are difficult to crack, including using different types of characters (uppercase, lowercase, numbers, special characters).
- Password Management – how to avoid storing passwords in unsecure places, such as paper notes, and how to use password managers for secure storage.
- The Three-Component Principle – explaining why a password should be of appropriate length, complexity, and uniqueness to ensure high security.
- The Role of Password Managers – discussing how password managers work and what benefits they offer, such as security and convenience in managing multiple passwords.
- Common Password Management Mistakes – how dangerous it is to reuse the same passwords across services or store them in unsecure files.
- Email Security Practices – how to avoid suspicious links and attachments, and how to use additional protection methods, such as encryption.

Appendix 5 | Worksheet "Creating Strong Passwords"
Create strong and secure passwords based on the following principles:

· Appropriate length (minimum 12 characters),
· Complexity (upper and lower case letters, numbers, special characters),
· Uniqueness (no obvious patterns, such as date of birth).

Individual work : Write down at least three different passwords:

Appendix 5 | Worksheet | Creating Strong Passwords

Work in pairs:

· After completing individual work, pair up with another participant.
· Show them your passwords.
· Ask them to mark (e.g. with a plus) whether the passwords meet all the criteria.
· The trainer can provide comments and suggestions for possible improvements.

Password 1

Length	**Notes**
Complexity	
Versatility	

Password 2

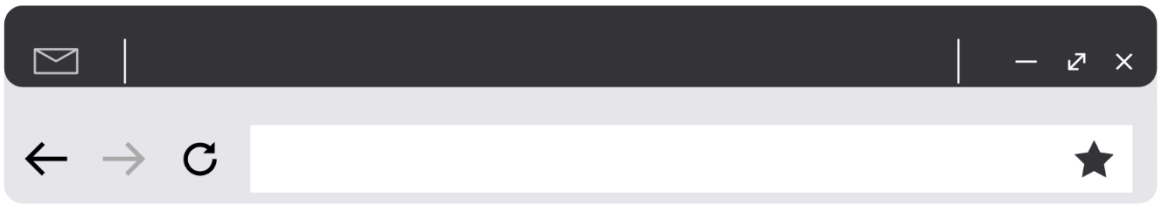
Length	**Notes**
Complexity	
Versatility	

Password 3

Length	**Notes**
Complexity	
Versatility	

Appendix 6 | Worksheet | Phishing Email Analysis

Read the emails below carefully. Identify the elements that indicate they are phishing emails.



Subject : **Urgent! Your account has been blocked!**

Dear user,

Due to suspicious activity on your account, your account has been temporarily blocked to protect your personal data. To avoid permanent blocking, please verify your account immediately.

Click here to verify your information and unlock your account: [Phishing link]

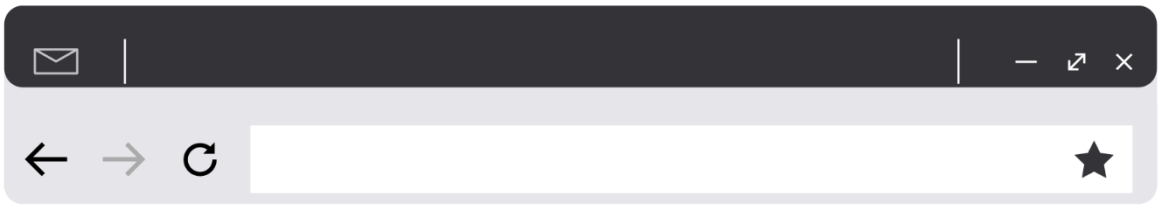
If you do not complete this action within 24 hours, your account will be permanently blocked. Please take quick action to avoid any inconvenience.

If you have any questions, please contact our technical support team.

Best regards,
Security Team
[Fake Company]

Appendix 6 | Worksheet | Phishing Email Analysis

Read the emails below carefully. Identify the elements that indicate they are phishing emails.



Subject : **Update Your Information! Your Account Requires Verification**

Hello [Name],

Your account at [Fake Company] requires an immediate update of your personal information. Due to a routine security check, we need to ensure that your data is up to date to grant you full access to our services.To update your information, click the link below and log in to your account:

[Phishing link – click here to update your information]

After clicking the link, you will be redirected to a page where you will need to enter your login credentials, credit card number, and other sensitive information.

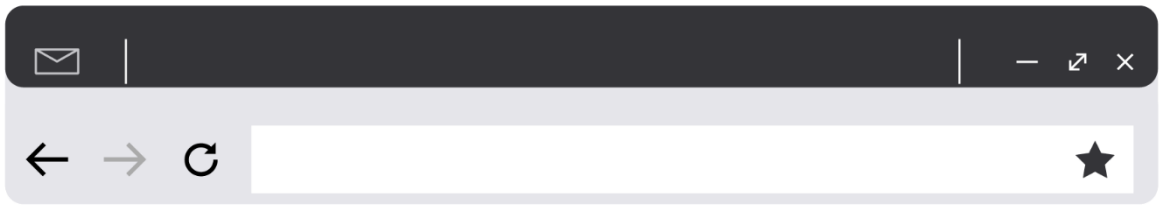
WARNING: If you do not update your information within 48 hours, your account will be permanently suspended.

Thank you for your understanding and cooperation.

Sincerely,
[Fake Company]
Team Customer Support

Appendix 6 | Worksheet | Phishing Email Analysis

Read the emails below carefully. Identify the elements that indicate they are phishing emails.



Subject : **Shipment confirmation - package could not be delivered**

Good day,

Your package could not be delivered due to incorrect address details. Please verify your details immediately so that we can re-attempt delivery.

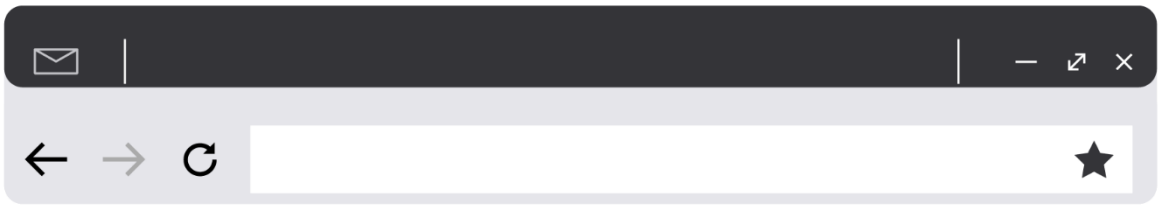
Click here to update your delivery details: [phishing link]

If you do not confirm your address within 24 hours, the package will be returned to the sender and you will incur additional costs.

Thank you for your quick response.
Shipping Team
[Fake Courier Company]

Appendix 6 | Worksheet | Phishing Email Analysis

Read the emails below carefully. Identify the elements that indicate they are phishing emails.



Subject : **You have received an e-gift card! Claim it now!**

Congratulations!

You have been selected as the winner of our random promotion. You receive an e-gift card worth PLN 500 to be used at [Popular Retail Network].

To claim your prize, click on the link below and confirm your details:
[phishing link - claim e-card]

Offer valid for 12 hours only.
Don't miss the opportunity!

Have a nice day!
Promotion Department
[Fake Company or Retail Network]

Appendix 7 | Recommendations for further reading and learning for participants

Cybersecurity websites: European and governmental organizations dealing with cybersecurity:

1) **ENISA (European Union Agency for Cybersecurity)**
   Website: https://www.enisa.europa.eu/
   ENISA is the EU agency dealing with cybersecurity, which publishes reports, guides and warnings on cyber threats.

2) **CERT-EU (Computer Emergency Response Team for the EU Institutions)**
   Website: https://cert.europa.eu/
   The organization monitors cyber threats and responds to cyberattacks on European institutions.

3) **EC3 – Europol Cyber Crime Centre**
   Website: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime
   Europol offers information on cybercrime and data security.

4) **NCSC UK (National Cyber Security Centre)**
   Website: https://www.ncsc.gov.uk/
   The UK government's cybersecurity portal, which offers guides, alerts and online courses for citizens, businesses and public institutions.

2.5 Module I - Pre/Post Test

1. Which of the following best describes “phishing”?

A) Installing updates to improve computer performance
B) A method of tricking people into revealing personal information through fake emails
C) A type of antivirus program
D) A process of encrypting data

2. Why are regular software updates important?

A) They make your computer slower
B) They change the design of your computer
C) They fix security vulnerabilities and protect against new threats
D) They remove antivirus software

3. What is the main function of a firewall?

A) To speed up your internet connection
B) To protect against unauthorized access to a network
C) To store passwords securely
D) To delete spam emails automatically

4. Which of the following is the most secure password?

A) password123
B) 12345678
C) MyDogIsCute
D) M@rK_82!x

5. What should you do if you receive an email from an unknown sender asking for personal data?

A) Reply with your information immediately
B) Click the link to check what it is about
C) Delete the email or report it as phishing
D) Forward it to your friends to warn them

6. What is “two-factor authentication (2FA)” used for?

A) It allows you to use two passwords at once
B) It adds an extra layer of security by requiring two forms of verification
C) It encrypts your emails automatically
D) It stores your login data

7. Which of the following statements about public Wi-Fi networks is TRUE?

A) They are always safe if the connection is free
B) You should avoid entering sensitive data when using public Wi-Fi
C) You can safely use them without a password
D) They automatically encrypt your data

8. What is the purpose of a VPN (Virtual Private Network)?

A) To improve the speed of your internet
B) To block pop-up advertisements
C) To provide a secure and private connection to the internet
D) To manage your passwords

9. Which of the following is an example of ransomware?

A) Software that encrypts your files and demands payment to unlock them
B) An antivirus program that scans your system
C) A tool for blocking spam emails
D) A firewall application

10. What is one good practice for protecting your privacy on social media?

A) Sharing your full address and phone number
B) Setting all posts to “public”
C) Reviewing and adjusting privacy settings regularly
D) Using the same password for all accounts

Answer Key Summary

1	**B**
2	**C**
3	**B**
4	**D**
5	**C**
6	**B**
7	**B**
8	**C**
9	**A**
10	**C**

MODULE II

Common Online Scams Targeting Seniors

3. Module II - Common Online Scams targeting Seniors

This four-hour module empowers seniors to recognize, understand, and protect themselves from online scams and cybersecurity threats. It addresses their unique vulnerabilities through practical strategies and preventive measures, fostering confidence in navigating digital technologies safely. Participants will learn how scams operate, identify warning signs in digital communications, and understand manipulation tactics like social engineering. The module covers common scams (phishing, smishing, vishing) and technical threats (malware, ransomware, spyware), offering strategies for protection. Additionally, it emphasizes personal data security, empowering seniors how to store, share, and back up sensitive information confidently.

3.1 Learning Objectives

The aim of this module is to enhance seniors' understanding of common online scams, the tactics used by scammers, and the importance of identifying and avoiding digital threats. To equip participants with practical skills and preventive measures to protect themselves from cybersecurity risks, including phishing, smishing, vishing, and malicious software. To build confidence and digital literacy among seniors by teaching them how to safeguard personal data, recognize manipulation tactics, and engage safely with digital technologies.

- Understanding how scams work and recognizing the psychological and technological methods used by scammers.
- Identifying suspicious content and differentiating legitimate from fraudulent communication.
- Gaining knowledge about common types of scams and learning strategies to protect themselves from cyber threats.
- Building confidence in safeguarding personal data, creating backups, and navigating digital tools securely.

3.2 Structure, Content & Learning Outcomes

On successful completion of this module, learners will be able to:

- Identify common techniques, technologies, and goals used in scams, and explain how scammers trick their targets.
- Recognize warning signs in digital content such as emails, SMS messages, websites, and advertisements, and differentiate between legitimate and suspicious communications.
- Define social engineering, identify common tactics used by scammers, understand why seniors are often targeted, and apply preventive measures to protect against social engineering attacks.
- Explain how scammers exploit emotions and common behavioral patterns in seniors, and apply strategies to remain calm and cautious when under emotional pressure.
- Identify the most common types of scams, including phishing, smishing, vishing, and fake identity or financial scams, and describe the manipulative techniques used in each.
- Identify different types of malicious software such as malware, ransomware, spyware, viruses, and trojans, describe methods for protecting against them, recognize dangerous pop-ups, close them safely, and use tools to block pop-ups and verify website safety.
- Define personal data, identify which types are valuable to scammers and how they are exploited, and apply best practices for securely storing and sharing personal data.
- Explain the importance of data backup, implement tips to reduce vulnerability to data loss, and build confidence in using technology safely.

3.3 Agenda I Detailed Session Plan

MODULE II
Common Online Scams Targeting Seniors

1st Session

Welcome
Duration *5 min*

Learning Objectives

- Introduce the topic and create a welcoming environment.

Content/ Method

- Brief introduction to the session, outline objectives and set expectations
- Set the stage for the training by outlining the module and its importance.

Material

- Whiteboard or flip chart for session objectives.
- Markers.
- Printed agenda or presentation slide outlining the session.

2nd Session

Icebreaker Activity: "Two Truths and a Scam"
Duration *10 min*

Learning Objectives

- After completing this activity, learners will be able to distinguish between accurate online safety practices and common misconceptions used in scams.

Content/ Method

- An interactive group exercise in the form of a game called "Two truths and a lie" aimed at presenting key concepts related to fraud and Internet safety. Participants analyze short statements, discuss them in pairs or small groups, and identify which one is false (a lie or a myth). The trainer provides quick feedback and clarifies any doubts.
- Participant receives a card with three statements and must decide which one is a scam. Then, the participant introduces themselves and, after giving their name, must read their statements and say which one they consider to be a scam. Everyone else will listen and indicate whether they agree or disagree. If someone disagrees, they stand up and explain which statement they consider to be a real scam. At the end, the trainer asks the participants if anyone has ever encountered any of these scams or heard about them.

Material

- Printed or digital list of statement sets (2 truths + 1 scam) – Appendix 1, 2
- Pen and paper (optional, for note-taking or group guesses)
- Whiteboard or screen (optional, for displaying answers and explanations)

3rd Session

Lecture 1: Recognizing Scams
Duration *30 min*

Learning Objectives

- Help participants understand the key mechanisms of scams, what are the tricks and goals of scammers.

Content/ Method

- The trainer uses slides to present the most common scams targeting older adults and explains the objectives and mechanisms of these scams. Finally, the trainer asks participants which mechanism frightens them the most.

Material

- Presentation slides covering different possible online scams targeting seniors.
- A projector and laptop for presentation delivery.
- Handouts summarizing different mechanisms of scams, their tricks used to reach these goals - Appendix 3.

Activity 1: Identifying Suspicious Content
Duration *15 min*

Learning Objectives

- Familiarize participants with the warning signs in emails, SMS messages, websites and advertisements.

Content/ Method

- Participants will be shown real screenshots of actual SMS messages, emails, websites, and dangerous popups. They will be asked to identify discrepancies and determine which examples are legitimate and which are scams. After each decision, an explanation will follow, clarifying why something is a scam and why something is not.
- The trainer shows pictures of two screenshots side by side and asks the group to identify the differences between the scam and the genuine example, and determine which one is the scam. The trainer continues in the same manner with all the examples, keeping the tone light and engaging to maintain the group's focus and participation. The trainer explains each pair of examples after participants have shared their thoughts. Ask them what was the hardest example to identify as a scam? Then, the trainer gives out handouts.

Material

- Presentation slides with visual examples of real and fake screenshots of SMS messages, emails, websites and popups.
- A projector and laptop for presentation delivery.
- Worksheets for participants to mark answers or write notes.
- Handouts with guidelines for recognizing fake examples from the real ones - Appendix 4.

Break | Duration *5 min*

- **Allow time for participants to recharge and reflect.**
- **Short break to refresh.**

4th Session

Lecture 2: Understanding manipulation
Duration *30 min*

Learning Objectives

- Help participants to understand social engineering.

Content/ Method

- Teach participants about Social Engineering - Overview of the most common tactics, reasons why scammers target seniors and how to protect yourself from this kind of scam. Define the situation in a way that if anyone finds him or herself in a social engineering scam they stay calm and collected and do not cave under pressure.
- The trainer presents examples of phishing and smishing messages that provoke fear and distress, followed by how they often suggest an easy and fast solution—like clicking a link and entering your bank details or personal information, or even following a series of commands so 'they' can fix the problem for you. Trainer ask participant what would they do in case of a social engineering attack?. The trainer hands out printed materials with additional information about social engineering tactics and how to recognize them.

Material

- Presentation slides explaining social engineering.
- A projector and laptop for live demonstrations of privacy settings.
- Printed handouts with a description of social engineering and guidelines to red flags and preventative measurements in case someone is targeted with this kind of scam - Appendix 5.

Activity 2: Social Engineering Live
Duration *20 min*

Learning Objectives

- Give participants the opportunity to experience different social engineering methods in a safe environment.

Content/ Method

- Participants will be presented with different scenarios where some of them are a form of social engineering and others are not. The social engineering scenarios will target their emotions and behaviors.
- Trainer ask participants to form five groups of tree. The trainer hands out the worksheets and gives instructions to the groups. Their task is to determine which of them are scams and which are genuine and write down the reasons behind their conclusions. Once the groups have reviewed all the scenarios and made their decisions, the trainer ask to share findings with the group. Trainer moderate discussion about the scenarios and ask participants why they think some are genuine and others are scams, what scenario would be the most fear-provoking if they were in it, and why.

Material

- Printed out handouts with different scenarios.
- Worksheet where participants note which scenarios are a scam and which not – Appendix 6.

Break | Duration *5 min*

- **Provide time to rest and prepare for the next session.**
- **A short break to refresh.**

5th Session

Lecture 3: Most common types of scams
Duration *30 min*

Learning Objectives

- To refresh scams that were already mentioned, a quick follow up overview of the most common scams such as smishing, vishing and phishing.
- Adding to the already given knowledge in former lectures malicious software.

Content/ Method

- A quick overview of the most common scams. Phishing, smishing, wishing, fake identities and money scams. Additionally informing participants about malicious software, what it is and how to detect it.
- The trainer explains the most important information about the most common scams and malware using slides. Then, they hand out materials describing them and discuss the materials with the training participants to make sure that everyone understands everything as clearly as possible. Finally, they ask if the participants know what signs to look for on the Internet.

Material

- Presentation slides showcasing examples of phishing, vishing, smishing scams.
- A projector and laptop for showing examples of the most common scams.
- Printed handouts detailing the most common scams and malicious software, what it is, how it can harm the victim and how to recognize it - Appendix 7.

Activity 3: Spot the Malicious Software
Duration *20 min*

Learning Objectives

- Develop the ability to recognize different types of malicious software.

Content/ Method

- Group activity where participants identify and discuss different types of malicious software through handouts.
- The trainer explains that participants will test their knowledge of malware in groups of three. The trainer hands out the scenarios and asks the participants to read them. The participants' task is to determine what type of software was used (Trojan, virus, adware, ransomware, or spyware) and answer the questions under each scenario. Each group shares its answers with the other groups. The trainer then distributes answer sheets and asks the participants to review the answers and analyze the key aspects of recognizing the software used and ways to protect against such an attack. Finally, the trainer asks which type of software they consider to be the most and least harmful.

Material

- Handouts with descriptions of malicious software.
- Worksheets for participants to write down what is the software for the given example and what it does to the device and what are the preventative measures for the given example.
- Participant Handout – Spot the Malicious Software - Appendix 8

Break | Duration 5'

- **Provide time to rest and prepare.**
- **Short break to refresh.**

6th Session

Lecture 4: Basic Data Protection and Data Backup
Duration *30 min*

Learning Objectives

- Participants will be able to define personal data and which data is valuable to scammers. They will also be aware of the importance of data backup.

Content/ Method

- Presentation with clarification of personal data. Participants will be educated on the topics of where it is safe to share data and where it is not, they will be informed of the importance of identifying data that can be used against them. Participants will also be informed about which data should be backed up and why.
- The trainer gives out printed materials and guides learners through the content using slides, explaining: personal information categories, what data can be harmful in the wrong hands and why, where we can share personal data online, what we should never share online, what backing up is, how backups can protect you from malware attacks, best practices for safe backups and tips to keep your data safe
- The trainer encourages discussion and asks participants if they have ever witnessed an attempted cyberattack using software or participated in such an attack. Finally, the trainer ask if they will now make backup copies of important data.

Material

- Presentation regarding personal data, where and what we can share online combined with the information needed about backing up data .
- Handouts with the guidelines about personal data, where to share where not to and why is it important that the important information is backed up - Appendix 9.

Activity 4: Backing up files to a cloud service and external memory storage.
Duration *20 min*

Learning Objectives

- This knowledge will help participants to backup files safely using verified cloud services end external hard drives.

Content/ Method

- Participants will backup dummy files to a cloud service familiar to them (Google Drive, Dropbox, iCloud, OneDrive). They will also backup the same dummy files to a USB drive.
- The trainer distributes materials containing information on backing up files to an external drive and to a cloud service. The trainer demonstrates on a screen or projector, and participants follow the process of copying files from a computer to an external drive and uploading files to a cloud service. The trainer helps those who need assistance. Question for reflection at the end: “Do you think you can back up your files on your own, or does anyone need additional information?”, “Is there anything you would like to ask or share your opinion about today's topic of online fraud?”

Material

- Dummy files so they can be backed up.
- Computers and USB drives.
- Laptop and a projector so the teacher can show an example of the process.
- Handouts with instructions on how to backup files on a external drive and to a cloud service - instructions tailored for all the major cloud providers-How to Backup Your Files - Appendix 10

7th Session

Discussion| Duration *10* min

Learning Objectives

- Encourage a proactive mindset full of awareness in regards to online scams.
- Summarize the training and ensure participants understand how to protect themselves from online scams.

Content/ Method

- Go over the key points of the most common online scams. Establish the awareness that if something is communicated in a extremely time sensitive manner to always be aware of a possible scam.
- Group discussion on how to handle a situation where one can find himself in an online scam. What are the key tell tale signs of some suspicious activities we might encounter and what to do in these kind of scenarios.
- The trainer summarizes the most important information on what to do if you fall victim to online fraud and lists the key signs of suspicious activity. The trainer thanks the participants and provides supporting materials, then distributes a checklist on how to recognize online fraud and what to do about it. The trainer ask the participants open-ended questions: "What is the most important thing you have learned today about online fraud and how to protect yourself from it?" "Do you feel more confident now in recognizing and avoiding scams?" "Is there a topic or question from today's session that you would like more information about?"

Material

- Whiteboard and markers for brainstorming ways to recognize scams.
- Handout: checklist regarding online scams - Appendix 11.
  Handouts Online safety checklist.

Wrap Up
Duration *5"*

Learning Objectives

- Summarize the session and encourage participants to continue practicing securely.

Content/ Method

- Final recap of key points, provide any additional resources for future learning.

Material

- Handouts with key points and resources.

3.4 Additional Information

3.4.1 Trainers' Self Reflection

- Did I effectively communicate the importance of online hazards?
- Did I ensure that participants understood the preventative measures?
- How did I engage the participants in the activities and discussions?
- Were the resources and materials helpful to the participants?

3.4.2 Trainers' Evaluation of the Program

- Is the content of the training relevant and clear for seniors?
- Were the activities and discussions effective in helping participants learn the material?
- Do the outcomes align with the module's learning objectives?

3.4.3 Materials, Additional Resources

Appendix 1 | Two truths & a scam

Set 1

- Scammers often pretend to be someone you trust.
- Legitimate companies will never email you.
- Phishing emails often create a sense of urgency.

Set 2

- You should never share your banking PIN with anyone.
- All websites that start with “https” are 100% safe.
- Scammers may use official-looking logos to trick you.

Set 3

- Ransomware can lock you out of your computer.
- Clicking unknown pop-ups can install malware.
- It’s safe to open any attachment from a friend without checking.

Set 4

- Social engineering often involves emotional manipulation.
- Government agencies always contact you by phone first.
- Seniors are often targeted due to perceived vulnerability.

Set 5

- It’s okay to reuse the same password for multiple accounts.
- A strong password includes letters, numbers, and symbols.
- Using two-factor authentication adds extra protection.

Set 6

- Scammers can fake caller ID to look like a real number.
- It’s safe to give your full address in an online giveaway.
- Always be cautious with unsolicited offers.

Set 7

Smishing is a scam sent via text message.

Malware only affects old computers.

Antivirus software helps protect against malicious attacks.

Set 8

Scammers may impersonate tech support.

You should click unknown links to check if they work.

Always check URLs before entering personal information.

Set 9

Fake job offers can be used to steal your personal info.

Scams only happen to people who aren't tech-savvy.

Online ads can sometimes lead to scam websites.

Set 10

Some scams ask for gift cards as payment.

It's safe to download apps from trusted app stores.

You should share your login info with close friends.

Set 11

Scammers sometimes use fear to pressure you.

Every pop-up warning is a real virus alert.

It's important to verify messages before acting.

Set 12

Legit companies don't ask for personal info via email.

Public Wi-Fi is always secure and safe to use.

Updating your device helps fix security vulnerabilities.

Set 13

Scams can happen on social media platforms.

Clicking “unsubscribe” in a scam email is harmless.

You should report suspicious activity to the platform.

Set 14

It’s okay to post your travel plans publicly online.

Scammers can monitor your social media posts.

Be cautious of friend requests from strangers.

Set 15

Backup copies protect your data in case of attacks.

You should ignore software update reminders.

Use strong, unique passwords for each account.

Appendix 2 | Correct Answers

Set 1

- True – Scammers often pretend to be someone you trust.
- False – Legitimate companies will never email you. (This is a myth. Legitimate companies may contact users via email, but they do not request sensitive personal or financial information.)
- True – Phishing emails often create a sense of urgency.

Set 2

- True – You should never share your banking PIN with anyone.
- False – All websites that start with “https” are completely safe. (This is a myth. “https” indicates encryption, not legitimacy.)
- True – Scammers may use official-looking logos to deceive users.

Set 3

- True – Ransomware can lock users out of their computers.
- True – Clicking unknown pop-ups can install malware.
- False – It is safe to open any attachment from a friend without checking. (This is a myth. Attachments from trusted contacts can also be infected.)

Set 4

- True – Social engineering often relies on emotional manipulation.
- False – Government agencies always contact individuals by phone first. (This is a myth. Official communication is often conducted by mail.)
- True – Seniors are frequently targeted due to perceived vulnerability.

Set 5

- False – It is acceptable to reuse the same password for multiple accounts. (This is a myth. Password reuse increases security risks.)
- True – Strong passwords include a combination of letters, numbers, and symbols.
- True – Two-factor authentication provides an additional layer of security.

Set 6

- True – Scammers can falsify caller ID information.
- False – It is safe to share your full address in online giveaways. (This is a myth. Personal information can be misused for scams.)
- True – Unsolicited offers should always be treated with caution.

Set 7

- True – Smishing refers to scams sent via text messages.
- False – Malware only affects old computers. (This is a myth. Any device can be affected.)
- True – Antivirus software helps protect against malicious threats.

Set 8

- True – Scammers may impersonate technical support services.
- False – Unknown links should be clicked to check if they are legitimate. (This is a myth. Clicking unknown links can be dangerous.)
- True – URLs should always be checked before entering personal information.

Set 9

- True – Fake job offers can be used to steal personal information.
- False – Scams only target people with low digital skills. (This is a myth. Anyone can be targeted.)
- True – Online advertisements can sometimes redirect users to scam websites.

Set 10

- True – Some scams request payment in gift cards.
- True – Downloading apps from trusted app stores is generally safer.
- False – Login details should be shared with close friends. (This is a myth. Login information should never be shared.)

Set 11

- True – Fear is commonly used by scammers to pressure victims.
- False – Every pop-up warning indicates a real virus threat. (This is a myth. Many alerts are fake.)
- True – Messages should always be verified before taking action.

Set 12

- True – Legitimate companies do not request personal information via email.
- False – Public Wi-Fi networks are always secure. (This is a myth. Public networks can expose personal data.)
- True – Regular software updates help fix security vulnerabilities.

Set 13

- True – Scams can occur on social media platforms.
- False – Clicking “unsubscribe” in scam emails is harmless. (This is a myth. It may confirm the user as an active target.)
- True – Suspicious activity should be reported to the relevant platform.

Set 14

- False – It is safe to publicly share travel plans online. (This is a myth. Such information can be exploited by scammers.)
- True – Scammers may monitor social media activity.
- True – Friend requests from unknown individuals should be treated cautiously.

Set 15

- True – Data backups protect information in case of cyberattacks.
- False – Software update reminders should be ignored. (This is a myth. Updates are critical for security.)
- True – Strong and unique passwords should be used for each account.

Appendix 3 | Mechanisms Used in Online Scams Targeting Seniors

1. Phishing (Email Scams)

Seniors receive emails that appear to come from trusted sources (banks, health services, etc.).

Trick: Fake links or login pages

Goal: Steal personal or financial information

2. Smishing (Text Message Scams)

Scammers send SMS messages with fake delivery notices, prize alerts, or warnings.

Trick: Urgent language + link to malicious site

Goal: Install malware or collect private data

3. Vishing (Voice Call Scams)

Phone calls from scammers pretending to be from a bank, tech support, or the government.

Trick: Fake caller ID + emotional pressure

Goal: Get banking info or remote access

4. Fake Websites (Spoofing)

Seniors are directed to fake websites that look like real ones (banks, shops, medical portals).

Trick: Slightly altered URLs (e.g., paypa1.com)

Goal: Capture login or payment info

5. Tech Support Scams (Email Scams)

Pop-ups or calls warn of a "virus" or computer issue, urging seniors to get help.

Trick: Fake error messages + requests for remote access

Goal: Control device or steal credit card data

6. Romance Scams

On social media or dating sites, scammers create emotional bonds to manipulate victims.

Trick: Fake photos, stories, and affection

Goal: Convince seniors to send money

7. Investment or Lottery Scams

Promises of huge returns or "you've won" messages that require upfront payment.

Trick: Fake documents, urgency, or official-sounding names

Goal: Get wire transfers, crypto, or gift cards

Appendix 4 | Spot the Scam: Quick Guidelines Handout

Use this checklist to help decide whether a message, email, website, or ad is real or fake.

1. Check the Sender or Source

- *Email address / phone number: Does the sender's info look suspicious or unfamiliar?*

✗ ***Fake:*** *support@paypal-secure123.com*
✓ ***Real:*** *support@paypal.com*

- *Misspelled brand names or strange URLs:*

✗ *netfflix-billing.com*
✓ *netflix.com*

2. Look for Urgency or Pressure

- Does the message try to scare or rush you?

  "Act now or your account will be locked!"
  "Final notice before legal action!"

Real companies don't threaten or pressure you like this

3. Examine the Language and Tone

- Look for spelling and grammar mistakes
- Is the tone too casual or too aggressive?
- Does it sound unnatural or translated?
  ✗ **Fake:** "Dear Customer, you account has be blocked urgently, kindly act now."
  ✓ **Real:** "We noticed unusual activity on your account. Please review it."

4. Check the Link Before Clicking

- Hover over links to see where they actually lead
- Does the URL match the real company's website?
  ✗ **Fake:** http://paypal.verify-now-support.com
  ✓ **Real:** https://www.paypal.com

5. Watch Out for Requests for Personal Info

Real companies never ask for:

- Passwords
- PIN codes
- Bank account or card numbers
- Social Security numbers

✗ "Please send your login info to verify your account."

✓ "We'll never ask for your password by email."

6. Look at Logos and Design

- Are logos blurry, stretched, or off-color?
- Is the layout strange or inconsistent?

Real companies use clean, professional, consistent design.

7. Too Good to Be True? Probably Is.

"You've won a new iPhone!"

"You've been selected for a $1,000 gift card!"

Real prizes don't ask for payment or sensitive info upfront.

✔ **Real or ✗ Fake?**

Ask yourself:

- **Do I trust the source?**
- **Am I being rushed or scared into action?**
- **Does anything feel off or unusual?**

When in doubt, don't click, don't respond, and report it!

Appendix 5 | Social Engineering Scams – What You Need to Know

What is Social Engineering?

Social engineering is when scammers use manipulation, pressure, and emotions to trick you into giving away personal information, money, or access to your accounts.

Dangers of Social Engineering

Scammers might pretend to be from trusted sources such as:

- Banks (e.g., “Your account has been locked!”)
- Courier services (e.g., “You missed a package. Pay now!”)
- Government agencies (e.g., “You owe unpaid taxes.”)
- The police or Department of Justice (e.g., “You’re under investigation.”)
- Tech support (e.g., “We’ve detected a virus on your computer.”)
- Family or friends (e.g., “I’m in trouble, please send money!”)

They will often create a sense of urgency or fear to make you act fast without thinking.

Red Flags to Watch Out For

- You are told to act **immediately** or face consequences
- You are asked for **personal information**, passwords, or banking details
- You are asked to **pay in gift cards**, **crypto, or wire transfers**
- Messages have **strange grammar or spelling**
- You’re being contacted out of the blue by someone you don’t know

Preventive Measures

Always do the following:

1. Stay calm. Take a moment to breathe and don't rush.
2. Never give out personal information via phone, email, or text.
3. Hang up or delete the message if it feels suspicious.
4. Verify the request yourself:

If someone claims to be from a bank, delivery company, government office, or tech support — always contact the organization directly.
Use their official website or phone number, not the one provided in the message or email.

Example:

- **Call your bank using the number on your bank card or official website**
- **Visit the official government site if you're unsure about tax-related messages**
- **Contact the courier company's official support to check if a package is real**

Remember:

- **Real companies do not threaten or pressure you**
- **Real institutions will never ask you for passwords or PINs**
- **Real messages will feel professional and respectful**
- **Scams rely on fear, confusion, and speed**

If something feels "off," pause and ask someone you trust. It's always better to double-check than to fall into a trap.

Appendix 6 | Scenarios: Spot the Scam

Scenario 1: Bank Urgency Message

You receive an email from what appears to be your bank. The subject line reads: 'URGENT: Account Access Issue'. The message claims that there has been suspicious activity on your account and that you must verify your personal and banking information immediately. It provides a link and warns that if you don't respond within 24 hours, your account will be permanently suspended.

Scenario 2: Phone Storage Full Alert

While browsing the internet or using an app, a pop-up message appears saying: 'Warning! Your phone storage is full. Tap here to clean your device and avoid data loss.' The message appears urgent, mimics your phone's system style, and when tapped, redirects you to download a third-party app that promises to optimize your device.

Scenario 3: Tech Support Call

You receive a call from someone claiming to be a Microsoft technician. They say your computer has been infected with a dangerous virus and it's sending error messages. They offer to fix it remotely and guide you through downloading software to give them access to your computer. Once connected, they 'scan' your computer and then demand payment to remove the virus, often asking for your credit card or online banking access.

Scenario 4: Utility Bill Payment Scam

You receive an email or text message that looks like it's from your electricity provider. It claims that your last payment failed and if you don't pay the outstanding balance within 12 hours, your electricity will be disconnected. The message includes a link to a payment page that looks very similar to the real utility website but asks for your credit card and personal details.

Scenario 5: Bank Transaction Notification

You receive an email from your bank with the subject: 'Transaction Confirmation – €74.60 at MERKUR'. The message confirms a transaction made today at 13:45. If you don't recognize the charge, it instructs you to call the bank's fraud department at the official number listed on their website. The email includes no clickable links and uses a calm and professional tone.

Scenario 6: Google Storage Warning

You receive an email from Google saying: 'Your Google Account storage is 98% full. You're currently using 14.8 GB of your 15 GB storage allowance. To continue receiving emails and using Google Drive, please manage or upgrade your storage.' The message contains two buttons: one to manage your storage and another to upgrade, both leading to official Google websites.

Appendix 7 | Common Online Scams & How to Protect Yourself

1. Smishing (SMS Phishing)

You receive a text message that appears to be from your bank, delivery service, or a government institution. It may claim there's an issue with your account or package and include a link.

Smishing: Phishing via text messages, often containing urgent messages that trick you into clicking on a link or providing personal information.

Red Flags:
- Urgent language ('your account will be closed')
- Suspicious links
- Asking for personal or banking info

What to do:
- Never click on links from unknown numbers.
- Contact the company directly using an official phone number or website.
- Block and report the sender.

2. Vishing (Voice Phishing)

You receive a phone call from someone pretending to be from your bank, police, or tech support. They ask for personal information or claim there's been suspicious activity.

Vishing: voice phishing, where scammers impersonate legitimate entities over the phone to steal information.

Variation: Fake voice using AI

Scammers can now mimic the voice of a loved one using AI. They might call pretending to be your grandchild or child, asking for urgent help or money.

Red Flags:
- Caller pressures you to act fast
- Emotional manipulation ('I'm in trouble!')
- Asks for money or info

What to do:
- Hang up and call the person back directly using a known number.
- Contact another family member to verify the story.
- Never give personal or banking info over the phone.

3. Phishing (Email Fraud)

You receive an email that looks official (from your bank, PayPal, tax office, etc.) asking you to confirm details, reset your password, or click a link.

Phishing: Fake emails or text messages that trick you into revealing confidential information (such as passwords or bank details).

Red Flags:
- Email contains grammar mistakes
- Uses fear ('unauthorized login detected')
- Requests personal info

What to do:
- Don't click on suspicious links.
- Check the sender's email address carefully.
- Contact the company through their official site.

4. Financial Fraud
Scammers pose as investment advisors, fake charities, or even romantic interests. They build trust and then ask for money, donations, or help.

Financial scams: scammers ask for money under false pretenses, often promising rewards or threatening consequences.

Red Flags:
- Too-good-to-be-true investment returns
- Emotional manipulation
- Unverifiable charities or causes

What to do:
- Never send money to people you haven't met in person.
- Always research the company or person.
- Consult a trusted family member or advisor before making financial decisions.

5. Fake Identities & Impersonation
Scammers may pretend to be someone they are not—such as a government official, bank worker, or even a family member. They use fake documents, emails, or AI-generated voices to trick people into giving away sensitive information or sending money.

Fake identities: Scammers create fake online profiles to build trust and manipulate victims into handing over money or personal information.

Red Flags:
- Unexpected requests for personal data or money
- Sense of urgency or emotional pressure
- Contact made through unofficial or suspicious channels

What to do:
- Always verify the identity by calling the real person or institution through official contact details.
- Do not be afraid to hang up and check first.
- When in doubt, ask someone you trust to help you assess the situation.

6. Malicious software, or malware,
Is any software designed to harm a computer or steal personal information. Scammers often trick users into downloading it through fake emails, links, or pop-up ads. Once installed, malware can steal passwords, lock files, and even take control of your device. Always be cautious of unknown links or attachments, and make sure your computer has up-to-date antivirus software to keep you protected.

Appendix 8 | Participant Handout – Spot the Malicious Software

Objective

Familiarize yourself with common types of malicious software (Viruses, Trojans, Spyware, Ransomware, Adware) by reading and analyzing these realistic scenarios.
For every scam write down which scam it is (trojan, virus, adware, ransomware, spyware) and answer the question).

Scenario 1

"You receive an email from a trusted friend with an attachment titled 'Important Document.' When you open it, your computer begins to slow down, and strange pop-ups start appearing."

Question: What type of malware do you think this is? How would you protect yourself?

Scenario 2

"You get a pop-up while browsing saying, 'Your device is outdated! Click here to download an update.' You click the link and unknowingly download malicious software disguised as an update."

Question: What is the danger here? What should you do instead?

Scenario 3

"You download a free photo-editing app from an unfamiliar website. Over time, you notice ads appear in your browser, and you start receiving unsolicited marketing emails."

Question: What do you think has happened? What should you do next?

Scenario 4

"After clicking a link in an email saying, 'Your Netflix subscription is about to expire, click here to confirm payment,' a message pops up telling you to pay a ransom to unlock your files."

Question: How can you tell this is a scam? What should you do if something like this happens?

Scenario 5

"After clicking a link in an email saying, 'Your Netflix subscription is about to expire, click here to confirm payment,' a message pops up telling you to pay a ransom to unlock your files."

Question: Is this a dangerous type of software? What's the solution to get rid of it?

Appendix 9 | Personal Data Protection

1. What Is Personal Data?

Personal data is any information that can be used to identify you, either directly or indirectly. This includes:

- **Basic data:** Name, surname, date of birth, address
- **Contact info:** Email address, phone number
- **Identification numbers:** ID number, tax number, passport number
- **Financial data:** Bank account numbers, credit card numbers
- **Login credentials:** Usernames, passwords
- **Health data:** Medical records, prescriptions
- **Biometric data:** Fingerprints, facial recognition, voice
- **Location data:** GPS tracking, IP address
- **Personal preferences:** Search history, social media activity

2. What Data Can Be Harmful in the Wrong Hands (and Why)?

Scammers and cybercriminals target specific data that can be used to:

- **Steal your identity**
- **Access your bank accounts**
- **Commit fraud in your name**
- **Manipulate you emotionally or financially**

Most valuable data to scammers:

- **Personal ID (passport, etc,) -** Used for identity theft or opening fraudulent accounts.
- **Login credentials -** Grants access to emails, social media, online banking.
- **Bank and credit card details -** Used for unauthorized purchases or fund transfers.
- **Phone numbers & emails -** Used for phishing, smishing, spam, and impersonation.
- **Social media content -** Used to build fake profiles or manipulate you.

3. Where Can We Share Our Personal Info Online?

It's important to know where and when it's safe to share personal data. Some platforms are trustworthy, while others pose higher risks.

Places where it is generally safe to share personal data (with caution):

- Verified online stores (e.g., Amazon, Zalando, Mimovrste): For purchases, only when the website has HTTPS encryption and secure payment methods.
- Official government websites (e.g., IRS, Social Security portals e- Government portals): For submitting documents, taxes, applications.
- Reputable service providers (e.g., your bank, healthcare provider): Only through their official websites or apps.
- Trusted email providers and cloud services (e.g., Gmail, Outlook, Dropbox): When setting up accounts, backing up data.

Always make sure the site is official, has HTTPS, and is well-known before submitting any information.

Places where you should be extremely careful or avoid sharing personal info:

- Unverified online shops or ads (often found through pop-ups or social media)
- Unknown surveys, online quizzes, or giveaways
- Unsecured public Wi-Fi networks
- Links in unsolicited emails or text messages
- Social media platforms, especially in comments or direct messages

Tip: Even when the platform seems familiar, always double-check the web address and avoid sharing sensitive data like ID numbers or financial info unless absolutely necessary and safe.

4. What Info Can We Share – and What We Should Never Share Online?

- **Can be shared (with caution):** First Name, City and non-specific location, General Interests or Hobbies, Professional info (e.g., job title) Public email (for work), Profile Photos
- **Must NEVER be shared online:** Passwords and PINs, Full address (exceptin verified government suites and web stores.), ID numbers, tax numbers, Bank or credit card details, Medical records or health info, Sensitive family details or travel plans

Rule of thumb: If the information could be used to access your money, identity, or private life, don't share it online, no matter who is asking.

5. Backing up your data means making a copy of important files, documents, photos, and settings in a safe and separate location. This could be on an external hard drive, a USB key, or a secure cloud storage service.

Why Backup Matters:

Your data can be suddenly lost or compromised due to:

- Device failure (e.g., computer crash, phone breaks)
- Theft or loss of your phone or computer
- Ransomware or malware attacks that lock or destroy your files
- Accidental deletion or formatting
- Natural disasters (fire, flood, etc.)

How Backup Protects You from Malware Attacks:

Malware such as ransomware can encrypt your files and demand a payment to unlock them. If you have a secure backup, you don't need to pay the ransom – you can reset your device and restore your files safely from the backup.

Similarly, viruses and trojans can damage your files or operating system. If your files are backed up, you can reinstall your system and restore your important data without losing anything.

Best Practices for Safe Backups:

- Use both local and cloud backup: Keep a copy on an external hard drive and one in a trusted cloud service (like Google Drive, Dropbox, iCloud, OneDrive).
- Encrypt sensitive backups: Use password protection or encryption for sensitive data.
- Backup regularly: Set a weekly or monthly schedule depending on how often you update your files.
- Disconnect external drives when not in use: If ransomware attacks, it may target connected drives too.
- Test your backups: Make sure your backup system works by trying to restore files occasionally.

6. Tips to Keep Your Data Safe

- Use strong, unique passwords (and change them regularly)
- Enable two-factor authentication (2FA)
- Keep software and antivirus updated
- Avoid clicking on suspicious links or attachments
- Don't share personal info over the phone or email unless verified
- Back up your data regularly (cloud or external hard drive)
- Be careful with public Wi-Fi – avoid logging into sensitive accounts
- Check your privacy settings on social media
- Think before you post – once it's online, it can be copied or misused

Appendix 10 | How to Back up Your Files

1. Backing Up Files to an External Drive

Step 1: Connect Your External Drive

- Plug in your external hard drive or USB stick into your computer using the appropriate cable or port.
- Ensure the device is recognized by your computer (check the "This PC" or "My Computer" folder for Windows, or the Finder for Mac).

Step 2: Select the Files You Want to Backup

- Open the folder containing the files you want to back up.
- You can select specific files or entire folders. To select multiple files or folders, hold down the Ctrl (Windows) or Cmd (Mac) key while clicking on the items.

Step 3: Copy the Files

- Right-click on the selected files and choose Copy (or use the keyboard shortcut **Ctrl+C** for Windows, **Cmd+C** for Mac).
- Navigate to the external drive in "This PC" (Windows) or Finder (Mac).
- Right-click on the external drive and choose Paste (or use **Ctrl+V** for Windows, **Cmd+V** for Mac) to copy the files over.

Step 4: Eject the External Drive Safely

- Once the files have been copied, make sure to safely eject your external drive to avoid damaging the files.
- On Windows, right-click the external drive in "This PC" and select Eject.
- On Mac, drag the external drive icon to the Trash, or click the eject button next to the drive in Finder.
- On your Apple device (Mac or iPhone), go to **Settings** and sign in with your Apple ID.
- On a Mac, you can access iCloud from **System Preferences** > **Apple ID** > **iCloud**.
- On iPhone, go to **Settings** > [Your Name] > **iCloud**.

2. Backing Up Files to a Cloud Service

Using Google Drive

Step 1: Sign in to Your Google Account

- Open a web browser and go to Google Drive.
- Sign in with your Google account credentials (or create a new account if you don't have one).

Step 2: Upload Files to Google Drive

- Click on the New button on the left sidebar.
- Select File upload or Folder upload depending on what you want to backup.
- Browse for the files or folders you want to upload and click Open.

Step 3: Organize Your Files (Optional)

- You can create folders in Google Drive to keep your backup organized. Click New > Folder, name the folder, and move files into it by dragging and dropping.

Step 4: Check the Upload

- Ensure that your files have finished uploading. Google Drive will show a status bar while the upload is in progress.

Using Dropbox

Step 1: Sign in to Your Dropbox Account

- Open a browser and go to Dropbox.
- Sign in or create a new Dropbox account if you don't already have one.

Step 2: Upload Files to Dropbox

- Once signed in, click on the Upload files button.
- Select the files or folders you want to back up from your computer and click Open.
- You can also drag and drop files directly into the Dropbox website.
- On iPhone, check your iCloud storage usage by going to Settings > [Your Name] > iCloud

Important Tips for Backing Up:

- Backup regularly: Make a habit of backing up your data at least once a week to ensure you don't lose important files.
- Use both local and cloud backups: Keep a copy of your data both on an external hard drive and in the cloud for extra security.
- Encrypt sensitive files: When storing sensitive data (e.g., financial records, personal documents), consider encrypting it before uploading it to the cloud or saving it on an external drive.
- Test your backup: Occasionally test your backup by restoring some files to make sure everything is working properly.

Backing up your files is crucial to ensuring your data is safe and recoverable in the event of a device failure, cyber-attack, or accidental deletion. Both external drives and cloud services offer reliable ways to store your data securely. If you have any questions, feel free to ask for assistance or help setting up your backup system!

Appendix 11| Online Safety Checklist

1. Personal Information Protection

- **Review the personal information you share online** – Always be cautious about what you post on social media and other platforms. Only share information that's necessary.
- **Keep sensitive information private** – Never share passwords, PINs, bank account numbers, or ID numbers online.
- **Use strong, unique passwords** for your accounts and change them regularly.

  Enable two-factor authentication on accounts where possible, especially for banking, email, and social media.

2. Recognizing Scams

- **Be aware of common online scams** – Learn to identify scams such as phishing, smishing, vishing, and financial frauds.
- **Red flags for scams**:
  - Urgent language (e.g., "Immediate action required!")
  - Requests for personal, banking, or login information
  - Suspicious links or phone numbers
  - Emotional manipulation or threats (e.g., "Your account will be closed")
- **Know the difference between legitimate and fraudulent requests** – Verify the authenticity of any phone call, email, or message you receive before responding.
- **In case of doubt, always contact the organization directly** using their official contact details to verify the claim.

3. Handling Scams and Malicious Content

- **Do not click on suspicious links or open attachments** from unknown senders. These can be phishing attempts or contain malware.
- **Report any suspicious emails, messages, or phone calls** to the appropriate authorities (e.g., SI-CERT in Slovenia).
- **Always double-check any financial request** (money transfers, credit card info) by calling the person or organization directly.
- **Be cautious of unsolicited phone calls**, especially if the caller pressures you for money or personal details. Hang up and call back using a known number.

4. Protecting Your Devices from Malware

- **Install and update antivirus software** to protect your device from viruses, malware, and spyware.
- **Avoid downloading apps or software** from unverified sources. Stick to official app stores (Google Play Store, Apple App Store).
- **Regularly back up your data** to an external drive or cloud service to prevent data loss from a potential attack.
- **Keep your software and devices updated** with the latest security patches.
- **Be cautious when using public Wi-Fi** – Avoid accessing sensitive accounts while connected to public networks.

5. Safe Online Shopping

- **Only shop on verified, trusted websites** – Look for a padlock symbol in the browser bar and "https" in the URL.
- **Use secure payment methods**, like credit cards, when shopping online, as they offer fraud protection.
- **Check reviews and ratings** before making a purchase from a new online store.

6. Backup Your Data

- **Back up important files** (documents, photos, contacts) regularly to an external drive or cloud service. This will protect your data from device failure or ransomware attacks.
- **Use a reliable cloud backup service** (Google Drive, Dropbox, OneDrive) for added security.
- **Create a backup schedule** so that you can ensure your data is always up to date and safe.

7. Social Media Safety

- **Be cautious about what you share** on social media platforms (Facebook, Instagram, etc.). Avoid sharing sensitive information like your full address, phone number, and financial details.
- **Adjust your privacy settings** to control who can see your posts and personal information.
- **Don't accept friend requests** or messages from strangers. If you don't know the person, it's safer to ignore the request.

8. How to Handle a Social Engineering Attack

- **Stay calm and do not act in haste** if you receive a suspicious message or phone call.
- **Never give personal information over the phone, email,** or **text unless you are sure of the identity** of the person you are talking to.
- **Verify the caller's identity** by calling back using official contact numbers (e.g., your bank's official number or the company's website).
- **Don't be pressured** – Scammers often create a sense of urgency to get you to act quickly. Take your time and verify the request.

9. Emergency Response

- **If you suspect a scam or if your personal information is compromised**, contact your bank or credit card company immediately to freeze your accounts.
- **Report scams to authorities** such as SI-CERT in Slovenia or local police if necessary.
- **Seek advice from a trusted friend or family** member if you are unsure about a situation.

10. Stay Informed

- Stay up-to-date on the latest scams – Subscribe to newsletters or alerts from trusted sources such as SI-CERT or other security platforms.
- Educate yourself regularly about online threats and how to protect yourself.

Remember:
The internet can be a great tool, but it's important to stay vigilant and informed about the potential risks. By following this checklist, you can significantly reduce your vulnerability and keep your personal information and devices safe. If you're ever in doubt, always ask for help or advice from someone you trust. Your safety and peace of mind are the top priority!

Appendix 12 | Recommendations for further reading and learning for participants

Cybersecurity websites: European and governmental organizations dealing with cybersecurity:

1) **OLAF - EUROPEAN ANTI - FRAUD OFFICE**
   Website: https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_en
   OLAF is an EU body that investigates fraud, corruption, and serious misconduct within EU institutions and funds.

2) **Victim Support Europe**
   Website: https://victim-support.eu/help-for-victims/info-on-specific-types-of-victims/fraud-victims/
   Victim Support Europe is a European umbrella organization that advocates for the rights of all victims of crime and provides support services through its network of national member organizations.

3) **EC3 – Europol Cyber Crime Centre**
   Website: https://www.europol.europa.eu/crime-areas/cybercrime
   Europol offers information on cybercrime and data security.

4) **CERT-EU (Computer Emergency Response Team for the EU Institutions)**
   Website: https://cert.europa.eu/
   The organization monitors cyber threats and responds to cyberattacks on European institutions.

3.5 Module II – Pre/Post Test

1. Which of the following is an example of safe internet behavior?

A) Sharing your personal address on social media
B) Using strong and unique passwords for each account
C) Accepting friend requests from unknown people
D) Clicking every link that looks interesting

2. What is a common risk when using social media?

A) Meeting new friends
B) Information overload
C) Oversharing personal information that can be misused
D) Updating your privacy settings regularly

3. Why should you verify the source before sharing information online?

A) To avoid spreading misinformation or scams
B) To increase the number of likes and followers
C) To improve your computer's performance
D) To change your profile security level

4. Which of these passwords is the strongest?

A) 123456
B) qwerty
C) Sunflower2025!#
D) password

5. What should you do if you receive a suspicious message from a friend's hacked account?

A) Click the link to see what it is
B) Report or block the account and inform your friend
C) Reply asking for more information
D) Ignore it completely

6. What does "digital footprint" mean?

A) The total amount of data stored on your computer
B) The record of your online activities and shared information
C) The password you use for your accounts
D) The software that protects your computer

7. Why is it risky to use the same password for all accounts?

A) It can make logging in too slow
B) If one account is hacked, others can be easily compromised
C) It saves too much time
D) It requires using password managers

8. What is the best way to protect your privacy on social media?

A) Set your profile to “public”
B) Share all personal details
C) Review and adjust privacy settings regularly
D) Use your real birthday and address in every post

9. What is a sign of a fake or scam website?

A) It starts with “https://”
B) It has spelling errors and unrealistic offers
C) It shows a lock symbol in the browser
D) It provides contact information

10. Why should you log out of your accounts on shared or public computers?

A) To make space for the next user
B) To prevent unauthorized access to your data
C) To save battery power
D) To update your password automatically

Answer Key Summary

1	**B**
2	**C**
3	**A**
4	**C**
5	**B**
6	**B**
7	**B**
8	**C**
9	**B**
10	**B**

MODULE III

Online Banking and Shopping Safety

4. Module III - Online Banking and Shopping Safety

The aim of this module is to empower seniors to confidently use online banking and shopping platforms by providing them with essential knowledge and practical skills for managing digital financial activities. The module strengthens participants' understanding of how online banking and e-commerce services function, while emphasizing safe and responsible practices to protect against fraud, scams, and cyber threats.

Through practical guidance and real-life examples, the module supports the development of digital literacy and encourages seniors to adopt secure habits when making online payments, managing accounts, and sharing personal information. By the end of the module, participants are better equipped to maintain financial independence, take advantage of digital services, and engage in online banking and shopping with confidence, safety, and autonomy.

In addition, the module addresses common fears and uncertainties seniors may experience when using digital financial services, aiming to reduce anxiety related to online transactions. Participants are guided to recognize trustworthy platforms, apply basic security checks, and respond appropriately to suspicious activities. By reinforcing confidence through practice and clear explanations, the module helps seniors feel more in control of their digital financial decisions and supports their long-term engagement with online banking and shopping in a safe and informed manner.

4.1 Learning Objectives

The main objective of this module is to equip seniors with the practical knowledge and skills necessary to safely use online banking and e-commerce platforms. The module focuses on building digital confidence while reducing fear and anxiety related to technology, enabling participants to manage financial transactions securely and independently. Participants will learn how to protect their personal and financial information, recognize online risks, and apply effective security practices in everyday digital financial activities.

- Understand online banking and e-commerce fundamentals that support safe navigation, account management, and digital transactions.
- Develop skills to create strong passwords and activate Two-Factor Authentication (2FA) in order to enhance the security of online accounts.
- Identify trustworthy online shopping platforms and sellers by recognizing security indicators such as HTTPS, padlock icons, customer reviews, and trusted payment methods.
- Recognize and avoid online fraud and financial scams, including fake websites, phishing attempts, and deceptive offers.
- Protect personal and financial data by using antivirus software, monitoring transactions, and setting alerts for suspicious activity.
- Apply safe internet practices when using public networks, including understanding the risks of public Wi-Fi and using VPNs to secure connections.
- Build digital confidence and financial independence by applying learned skills to real-life online banking and shopping situations with reduced anxiety and increased trust in digital tools.

4.2 Structure, Content & Learning Outcomes

On successful completion of this module, learners will be able to:

- Understand how online banking works, learn about the benefits of managing accounts online, and get an overview of popular banking platforms.
- Navigate e-commerce websites, learn about the benefits of online shopping and popular platforms.
- Set up strong passwords and two-factor authentication (2FA): tips for creating strong passwords and using 2FA to increase security.
- Use banking apps and websites safely: use only official apps/websites, check for secure connections (https).
- Shopping on trusted websites: verify the authenticity of a website and understand reviews and ratings.
- Recognize secure payment options: identify secure payment methods (credit cards) and avoid unsecured payments (bank transfers).
- Secure devices: how to use antivirus software and update software.
- Use public Wi-Fi networks safely for financial transactions: risks associated with public networks and using VPNs to ensure security.

4.3 Agenda I Detailed Session Plan

MODULE III
Online Banking and Shopping Safety

1st Session

Welcome
Duration *5”*

Learning Objectives

- Introduce the topic and create a welcoming environment.

Content/ Method

- Brief introduction to the session, outline objectives and set expectations. Set the stage for the training by outlining the module and its importance.

Material

- Whiteboard or flip chart for session objectives.
- Markers.
- Printed agenda or presentation slide outlining the session.

2nd Session

Icebreaker Activity: " My First Online Banking Moment"
Duration *10*"

Learning Objectives

- Build connection through shared experiences and introduce the topic.

Content/ Method

- The trainer asks participants to share a brief story about their first experiences with online banking, including what they did and how they felt. As participants share their experiences, the trainer actively listens and writes down key feelings and thoughts on a flipchart or whiteboard (e.g., nervousness, excitement, confusion), visually capturing the group's shared experiences and emotions. Finally, the trainer briefly summarizes the shared emotions and experiences that participants have shared.

Material

- Flip chart or whiteboard to write keywords (e.g., nervous, excited), markers.

3rd Session

Lecture 1: Understanding Online Banking and Shopping Basics
Duration *30*"

Learning Objectives

- Help participants understand how online banking and shopping work, and distinguish safe vs. unsafe platforms.

Content/ Method

- The trainer discusses user-friendly examples such as Monzo or Revolut (banking) and Zalando or Coolblue (shopping), highlighting key features such as security, navigation, and usability. To reinforce their learning, participants compare a real website with a fake one, using their knowledge to spot signs of credibility and fraud.
- The trainer introduces the basics of online banking and shopping using screenshots and live demonstrations. The trainer guides participants through a simple banking platform, explaining how online banking works and showing them how to check their balance, transfer money, and use other basic features. The trainer then does the same for a shopping site, showing participants how to navigate the platform, select products, and proceed with the purchase process. The trainer displays two websites - one secure and one fake - and asks participants to identify which one is secure and explain why, encouraging them to apply their knowledge of website security. At the end, the trainer discuss the key takeaways from the session: the importance of checking for secure connections (HTTPS), recognizing legitimate platforms, and ways to avoid scams.

Material

- PowerPoint Presentation, visual handouts,
- Laptop, projector.

Activity 1: Platform Exploration
Duration *20"*

Learning Objectives

- Practice using online platforms and identifying key features.

Content/ Method

- The trainer divides the participants into pairs and gives each pair one task card, informing them that each card contains instructions on what to look for during the exercise, e.g., recognizing security features on a banking or shopping website. Once the exercise begins, the trainer circulates around the room, observing the participants, giving tips, and answering questions. The trainer also helps participants focus on key security elements such as padlock icons, 2FA settings, "https" addresses, or secure payment symbols to ensure they understand how to recognize security features. After the exercise, the trainer will ask each pair to briefly share what they discovered during their investigation. The trainer encourages a short discussion by asking questions such as, "What was easy and what was difficult about the task?" and "What made you consider a website or app to be safe or unsafe?" This will help participants reflect on their experiences and deepen their understanding of what makes an online platform safe.
- Finally, the trainer provides additional resources by sharing links to short articles or videos on online platform safety. Printed materials containing examples of safe and unsafe elements of websites/apps will also be distributed to serve as reference materials and reinforce the knowledge gained during the exercise.

Material

- Printed task guides to participants.
- Tablets, laptops, or large printed screenshots with demo versions of banking or shopping platforms.

Break | Duration *5'*

- **Allow time for participants to recharge and reflect.**
- **Short break to refresh.**

4th Session

Lecture 2: Secure Online Banking Practices
Duration *30"*

Learning Objectives

- Help participants how to create strong passwords and monitor accounts.

Content/ Method

- The trainer begins with a presentation covering key security practices in online banking. Topics to be discussed include creating strong passwords, enabling two-factor authentication (2FA), and setting up account alerts. The trainer will include real-life examples or short stories about online banking fraud during the lecture. Using real-life fraud cases, the trainer highlights common threats and shares practical security tips. One such case is the “Safe Account” scam reported in Ireland, which helps illustrate how fraud works in practice. They are encouraged to apply these steps on their own devices, making the session practical, useful, and immediately actionable.
- The trainer explains to participants why secure online banking is essential and how often security breaches occur. They highlight the potential risks and show how simple precautions can protect participants from fraud. Using a password strength checker, the trainer demonstrates in real time the difference between weak and strong passwords. The trainer asks participants to suggest sample passwords and tests them live to emphasize the importance of creating strong, unique passwords. He then demonstrates how to enable 2FA using screenshots or live simulations. The trainer explains the role of 2FA in preventing unauthorized access and guides participants through the process of enabling it. Next, the trainer will explain how to monitor banking activity and set up alerts for suspicious transactions. Using screenshots or a sample banking app, the trainer will walk participants through the steps to set up these alerts, emphasizing the importance of staying vigilant about account activity. During the Q&A session, the trainer will ask participants to share their experiences or concerns about online banking security. Finally, the trainer will distribute printed checklists summarizing safe online banking habits, which will be a useful resource for participants.

Material

- Presentation, password strength demo tool.
- Printed checklist.

Activity 2: Secure Your Online Banking
Duration *20*”

Learning Objectives

- Participants practice setting up 2FA and monitoring transactions in a simulated banking environment.

Content/ Method

- The trainer divides participants into pairs or small groups. Each group will work on laptops or smartphones with demo apps or banking platforms installed, as Revolut or Monzo. The trainer guides participants through the process of enabling 2FA: Using a step-by-step guide, they help participants complete the 2FA setup process on the demo platform. They walk around the room to offer assistance and ensure that everyone is following the steps correctly. The trainer then asks participants to check for any unauthorized transactions and helps them set up alerts for suspicious activity. They make sure participants understand the process and perform these steps on their demo platform.

- After the exercise, ask each group to share their experiences: “What challenges did you encounter when setting up 2FA?” “Were you able to find and set up transaction alerts? Which steps were helpful, and which were difficult?” Provides feedback: Emphasizes the importance of enabling 2FA and monitoring transactions for online banking security.

Material

- Laptops or smartphones.
- Demo banking app.
- Step-by-step guide to setting up 2FA and viewing transactions.

Break | Duration *5’*

- **Provide time to rest and prepare**
- **A short break to refresh.**

5th Session

Lecture 3: Safe Online Shopping
Duration *30”*

Learning Objectives

- Help seniors understand how to evaluate websites, identify secure payment options, and recognize fraudulent sellers.

Content/ Method

- During the lecture, the trainer explains how to recognize secure websites for online shopping and verify the authenticity of sellers. The trainer explains how to recognize secure websites, focusing on the HTTPS protocol, padlock icons, and other security symbols. They present examples of good and bad websites to show how to assess their credibility. The trainer also shows how to read reviews and check if sellers are genuine. At the end of the lecture, the trainer asks participants questions such as “What does the HTTPS protocol say about website security?” and “How can you check if an online seller is trustworthy?” to reinforce key concepts and engage participants.
- At the end, the trainer encourages participants to share their experiences with online shopping or their concerns about safe online shopping. Any challenges that participants may have encountered while shopping online will be discussed, and the trainer will answer any questions they may have.

Material

- Printed shopping examples, website screenshots.

Activity 3: Shopping from Trusted Websites
Duration *20"*

Learning Objectives

- Participants learn how to evaluate online stores for safety and verify payment methods.

Content/ Method

- In groups, participants first familiarize themselves with the store's legitimate website to identify key security features (e.g., HTTPS, trust seals, secure payment options). Next, using a presentation or pre-recorded video, they are shown examples of fake websites or suspicious online activity. The exercise focuses on helping them recognize common warning signs and compare safe and unsafe websites.
- The trainer divides participants into small groups and gives them a list of websites to review. Each group evaluates the websites for safety, focusing on indicators such as HTTPS protocol, secure payment methods, and credible reviews. The trainer walks among the groups, providing assistance as needed and offering guidance if the groups need help identifying warning signs such as suspicious reviews or unsafe website elements. At the end, the groups share information about the websites that were deemed safe and justify their assessment.

Material

- Computers with internet access.
- List of shopping websites.

Break | Duration 5'

- **Provide time to rest and prepare.**
- **Short break to refresh.**

6th Session

Lecture 4: Protecting Personal and Financial Information
Duration *30"*

Learning Objectives

- Equip seniors with knowledge on keeping devices secure, using antivirus software, and securing Wi-Fi connections.

Content/ Method

- The trainer gives a lecture explaining the concepts of antivirus software, VPNs, and safe web browsing. The presentation will include slides with key information and examples for each topic, highlighting best practices for device security. The trainer shows how to update devices, install antivirus software, and manage privacy settings to improve security. They show a short instructional video demonstrating the proper use of a VPN for secure web browsing. Throughout the lecture, the trainer will encourage participants to actively participate and make the session interactive by asking questions and providing real-life examples of how to

stay safe online. After the lecture, participants will have the opportunity to ask questions and clarify any doubts they may have about device security and online protection.

- Finally, the trainer will share simple, everyday practices for protecting personal data, such as avoiding suspicious links, not sharing too much information on websites, and recognizing common online traps. These steps help participants build safer digital habits.

Material

- Presentation slides, video tutorial on VPNs.

Activity 4: Securing Your Devices
Duration *20"*

Learning Objectives

- Participants practice installing antivirus software, using VPNs, and managing privacy settings.

Content/ Method

- Participants work in groups to install antivirus software, enable VPN for secure web browsing, and check privacy settings in apps and social media. This hands-on exercise helps them apply practical steps to protect their devices and personal data online.
- The trainer divides participants into small groups or pairs and provides them with laptops, antivirus software, and VPN applications to use during the exercise. Each group will follow step-by-step instructions provided by the trainer to install antivirus software, enable a VPN for secure web browsing, and check privacy settings in apps and social media accounts. The trainer circulates among the groups, offering assistance as needed and ensuring that all participants can successfully complete the tasks. The trainer also guides the groups through the process of identifying key privacy settings on their devices and social media profiles that enhance security. After the exercise, the trainer asks participants to share their experiences with securing their devices and privacy settings.

Material

- Laptops, antivirus software, VPN app

7th Session

Discussion | Duration *10"*

Learning Objectives

- Reflect on the key takeaways from the session and clarify any questions.

Content/ Method

- Group discussion during which participants share their experiences and conclusions. The trainer answers any remaining questions. Encourages participants to continue practicing the skills acquired during the session.

Wrap Up
Duration *5”*

Learning Objectives

- Summarize the session and encourage participants to continue practicing securely.

Content/ Method

- The trainer summarizes the session, highlighting the most important issues discussed. Participants will be encouraged to continue practicing the skills they have acquired through their personal online activities. The trainer thanks the participants for their participation and encourages them to use the knowledge they have gained to ensure their safety on the Internet.

Material

- Handouts with key points and resources.

4.4 Additional Information

4.4.1 Trainers' Self Reflection

- What aspects of the training went particularly well?
- Which parts of the session were most challenging for me to deliver?
- How engaged and responsive were the participants throughout the activities?
- Were participants able to meet the learning objectives? If not, why?
- What adjustments could improve the session in future iterations?

4.4.2 Trainers’ Evaluation of the Program

- Was the training content relevant to the needs of seniors and adapted to their level of knowledge and digital experience?
- Did participants understand the basic principles of online banking, e-commerce, cybersecurity, and online privacy?
- Were practical exercises, quizzes, and demonstrations effective in reinforcing learning and building digital confidence?
- Did discussions and reflections allow participants to deepen their understanding of secure online practices?
- Were the intended learning outcomes achieved, such as the ability to create strong passwords, recognize fraudulent websites, monitor transactions, and configure security settings?
- Did participants demonstrate increased confidence and independence in performing online banking and shopping tasks?
- Which aspects of the training were most successful, and which areas could be improved for future sessions?

4.4.3 Materials, Additional Resources

Appendix 1 | Characteristics of Strong Passwords

To ensure your online accounts are secure, your password should have the following characteristics:

- At least 8 characters – the longer, the better
- A mixture of uppercase and lowercase letters
- A combination of letters and numbers
- Inclusion of at least one special character, e.g., !, @, #, ?,]
- Note: Do not use < or > in your password, as these can cause problems in web browsers
- Detailed handouts are below !

Online Banking and Shopping Safety
Characteristics of Strong Passwords
Why Strong Passwords Matter

Creating strong passwords is a key step in protecting your personal and professional data. Weak passwords make it easier for hackers to access your accounts.

Use the following guidelines to build secure passwords:

Characteristics of Strong Passwords

- At least 8 characters – the longer, the better.
- A combination of uppercase and lowercase letters.
- A mixture of letters and numbers.
- At least one special character, such as: !, @, #, ?,].
- Avoid using < or > in your password, as these can cause issues in some web browsers.
- Additional Tips
- Do not use personal information (like your name or birth date).
- Use a unique password for each account.
- Consider using a trusted password manager.
- Change passwords regularly and avoid reusing old ones.

Practice Section (Optional)
Create a strong sample password using the tips above:

Rate your password strength:

WEAK	FAIR	STRONG

Appendix 2 | Step-by-Step Instructions for 2FA and Alerts

Part I: *Set Up Two-Factor Authentication (2FA)*

Purpose: *2FA provides extra security by requiring both your password and a second verification method (e.g., code sent to your phone).*

Steps:

1. *Open the demo banking app or platform on your device.*
2. *Go to Settings → Security Settings.*
3. *Tap Enable Two-Factor Authentication (2FA).*
4. *Choose your verification method:*
   - *SMS Code*
   - *Authenticator App (e.g., Google Authenticator)*
5. *Follow the instructions (enter the verification code you receive).*
6. *Confirm that 2FA is active and working.*

Part 2*: Review Transactions & Set Up Alerts*

Purpose: *Monitoring your transactions and setting up alerts helps you detect suspicious activity early.*

Steps:

7. *Navigate to Transaction History in the app.*
8. *Review recent transactions.*
9. *Identify and flag anything unfamiliar.*
10. *Go to Notifications or Alerts Settings.*
11. *Enable alerts for:*
    - *Large or unusual transactions*
    - *Logins from new devices*
    - *Changes to your account settings*

Key Reminders

- *Enable 2FA on all financial apps.*
- *Regularly check your transaction history.*
- *Use alerts to get notified about unusual activity.*

Appendix 3 | Recognizing security elements on banking and online shopping platforms

Task 1. Find the account balance

Try to locate the place where you can check the account balance.

- Where is it located? .....
- How is it labeled (e.g., “Balance”, “Account overview”, “Available funds”)? .....

Task 2. Find the payment option

Try to find where you can make a payment or complete a purchase.

- What is the name of this option?
  ☐ Transfer
  ☐ Pay
  ☐ Cart / Checkout
  ☐ Other: .....
- Was it easy to find?
  ☐ Yes
  ☐ No
  Why? .....

Task 3. Identify website security features

Look carefully at the website and mark the elements that indicate it is secure.

☐ lock icon in the browser address bar
☐ address begins with **https**
☐ recognizable payment system logos (e.g. Visa, Mastercard, PayPal, BLIK)
☐ additional payment confirmation (SMS code, banking app)
☐ privacy policy information

Did you notice anything else? .....

Task 4. Look for potential warning signs

Did you notice anything that might indicate the website could be unsafe?

☐ no lock icon
☐ suspicious website address
☐ too many pop-up windows
☐ requests for too much personal information
☐ other: .....

Task 5. Check additional security settings

Look for information about additional account or payment protection.

Did you find:
☐ two-factor authentication (2FA)
☐ SMS verification
☐ confirmation through a banking app

Where is this option located? .....

Exercise Summary:
What was the easiest part of the task? .....
What was the most difficult part? .....
What helps you recognize that a website or application is secure? .....

Conclusion: Using online banking and shopping platforms safely requires paying attention to website security indicators, the web address, and the way payments are confirmed.

Remember: If something on a website makes you feel unsure or suspicious, **do not enter your personal data and stop the process.**

Appendix 4 | Recommendations for further reading and learning for participants

Cybersecurity websites: European and governmental organizations dealing with cybersecurity:

1) **How to Set Up Two-Factor Authentication on All Your Online Accounts**
   Website: https://www.loginradius.com/blog/identity/how-to-setup-2fa-in-online-accounts/
   This comprehensive guide explains the importance of two-factor authentication (2FA) and provides step-by-step instructions for setting it up on various online accounts, including email, social media, and banking platforms.
2) **Setting Up 2-Factor Authentication | Technology Support Services**
   Website: https://it.nmu.edu/docs/setting-2-factor-authentication
   This resource from Northern Michigan University's IT department outlines the process for enabling two-factor authentication (2FA) on NMU services such as MyNMU and MyUser.
3) **Bank of Ireland Warning of Spike in 'Safe Account' Scam**
   Article: https://www.rte.ie/news/business/2025/0606/1517043-spike-in-safe-account-scam-warning-boi/
   This news article reports a significant increase in reports of 'safe account' scams in Ireland, with a tenfold rise in the past week. The Bank of Ireland warns consumers about this type of scam, where fraudsters trick individuals into transferring money to 'safe' accounts under false pretenses, highlighting the importance of vigilance and secure banking practices.
4) **National Cyber Security Centre – Shopping Online Securely**
   Website: https://www.ncsc.gov.uk/guidance/shopping-online-securely
   This official UK government guidance provides practical tips for consumers to shop safely online. It covers areas such as verifying the legitimacy of online stores, using secure payment methods, protecting personal information, and reporting suspicious activities.

5) **How to Create a Strong Password**
   Video: https://www.youtube.com/watch?v=_wQTRMBAvzg
   This video provides practical tips for creating strong and memorable passwords. It emphasizes the importance of using a combination of letters, numbers, and symbols, avoiding common mistakes, and considering passphrases as a secure alternative.
6) **TechRadar – Virtual Private Networks (VPNs)**
   Website: https://www.techradar.com/vpn/virtual-private-networks
   This comprehensive guide from TechRadar explores the concept of Virtual Private Networks (VPNs). It explains how VPNs work, their benefits for online privacy and security, and provides recommendations for top VPN services based on expert testing.

4.5 Module III – Pre/Post Test

1. What does "HTTPS" indicate in a website address?

A) The website is hosted in another country
B) The website is secure and data is encrypted
C) The website offers discounts
D) The website requires a login

2. Why is it important to use Two-Factor Authentication (2FA) for online banking?

A) It speeds up online transactions
B) It allows you to log in from multiple devices at once
C) It provides an extra layer of security by requiring two verification steps
D) It replaces the need for a password

3. What is the main benefit of using antivirus software?

A) It makes your computer faster
B) It protects against malware and phishing attacks
C) It helps manage online passwords
D) It blocks access to all online shopping websites

4. Which of the following passwords is the most secure?

A) Shopping2024
B) 12345678
C) Mybankpassword
D) H@ppy$hopper92!

5. What should you do if you see an online offer that looks "too good to be true"?

A) Share it with friends immediately
B) Click the link to check the details
C) Avoid it and verify the website before taking any action
D) Provide your details to claim the offer quickly

6. What is a safe payment method for online shopping?

A) Paying with a credit card on a secure website
B) Sending money through a direct wire transfer
C) Sharing your card number via email
D) Using any method if the website looks professional

7. Why should you avoid using public Wi-Fi for financial transactions?

A) It is too slow for online banking
B) It may be unencrypted and allow hackers to steal your data
C) It doesn't support secure websites
D) It blocks access to bank apps

8. What does a padlock icon in the browser's address bar mean?

A) The website is under maintenance
B) The connection between your device and the website is secure
C) The website requires cookies
D) The website is not trustworthy

9. How can you identify a trustworthy online shopping website?

A) It requests your password by email
B) It contains spelling errors and unclear contact details
C) It has HTTPS, a padlock icon, and verified customer reviews
D) It offers free items without payment

10. What should you do to protect your device and financial information?

A) Disable antivirus software to make your computer faster
B) Keep your software updated and use a VPN on public networks
C) Avoid checking your transaction history
D) Use the same password for all your accounts

Answer Key Summary

1	**B**
2	**C**
3	**B**
4	**D**
5	**C**
6	**A**
7	**B**
8	**B**
9	**C**
10	**B**

MODULE IV

Safe and Responsible Social Media Use for Seniors

5. Module IV - Safe and Responsible Social Media Use for Seniors

The “Safe Use of Social Media” module introduces seniors to responsible and secure engagement with social media platforms by combining essential knowledge with practical guidance. Participants learn how to set up and manage accounts, adjust privacy settings, recognize common online scams, and communicate safely, enabling them to participate in digital social spaces with greater confidence and control.

The module includes practical activities that help participants identify suspicious messages, fake profiles, and misleading links commonly found on social media. It also focuses on protecting personal information and digital identity through effective privacy management, limited data sharing, and secure account practices such as strong passwords and two-factor authentication. Guidance on device security, software updates, and safe internet connections is also provided.

By integrating these elements, the module ensures that seniors not only understand social media–related risks but also develop practical skills to manage them effectively. Participants complete the module with increased digital awareness, confidence, and the ability to apply safe social media practices in everyday online interactions.

5.1 Learning Objectives

The aim of this module is to enhance seniors' understanding and skills for safe, responsible, and meaningful engagement with social media. Through this training, seniors aged 65 and above will:

- Gain confidence in navigating popular social media platforms.
- Understand the importance of privacy settings and learn how to adjust them effectively.
- Identify and avoid common online scams and threats on social media.
- Develop habits for secure and responsible sharing of personal information online.
- Engage responsibly with social media content while ensuring their safety and well-being.

5.2 Structure, Content & Learning Outcomes

On successful completion of this module, learners will be able to:

- Identify key features and uses of popular platforms like Facebook, Instagram, and LinkedIn.
- Demonstrate the ability to create social media accounts using secure methods, such as choosing strong passwords and enabling two-factor authentication.
- Customize privacy settings to control visibility of personal information and posts.
- Manage contact settings to restrict unwanted messages and connection requests.
- Identify warning signs of scams such as phishing, fake profiles, and fraudulent links.
- Implement strategies to protect sensitive personal data from malicious actors.
- Review and modify previously shared content to align with best practices for online safety.
- Develop habits for securely sharing information, including avoiding oversharing or sharing sensitive content.

5.3 Agenda I Detailed Session Plan

MODULE IV
Safe and Responsible Social Media Use for Seniors

1st Session

Welcome
Duration *5'*

Learning Objectives

- Introduce the topic and create a welcoming environment.

Content/ Method

- Brief introduction to the session, outline objectives and set expectations
- Set the stage for the training by outlining the module and its importance.

Material

- Whiteboard or flip chart for session objectives.
- Markers.
- Printed agenda or presentation slide outlining the session.

2nd Session

Icebreaker Activity: Social Media Bingo
Duration *5'*

Learning Objectives

- Encourage participant interaction and start thinking about their digital habits.

Content/ Method

- As participants introduce themselves, they will mark off any terms they are familiar with. The first participant to complete a row on their bingo card will win a small prize. This will encourage participants to share their experience with social media and spark conversation around their digital habits.

Material

- Print out cards with common social media terms, such as "Facebook," "Instagram," "Like," "Hashtag," "Comment," "Follow," "Profile," etc
- Pens and pencils, highlighter and/or stickers

3rd Session

Lecture 1: Overview of Social Media
Duration *30'*

Learning Objectives

- Help participants understand the key functions and types of social media platforms.

Content/ Method

- Present an overview of popular platforms (Facebook, Instagram, Twitter, etc.), explaining their basic features and functionalities. Explain their features, benefits, and potential risks and how to securely set up an account

Material

- Presentation slides covering popular social media platforms, their features, and security risks.
- A projector and laptop for presentation delivery.
- Handouts summarizing features and security tips for Facebook, Instagram, and Twitter.
- Internet connection for live demonstrations of platform features.

Activity 1: Platform Familiarization
Duration *20'*

Learning Objectives

- Familiarize participants with how to navigate social media platforms.

Content/ Method

- Hands-on exploration of platforms (e.g., Facebook, Instagram, Twitter). Participants will practice setting up a social media account with emphasis on security (e.g., choosing strong passwords, enabling two-factor authentication).

Material

- Computers, tablets, or smartphones for participants to explore platforms.
- Printed guides on setting up accounts securely, including: *Instructions on creating strong passwords. Steps for enabling two-factor authentication*

Break | Duration *5'*

- **Allow time for participants to recharge and reflect.**
- **Short break to refresh.**

4th Session

Lecture 2: Privacy Settings
Duration *30'*

Learning Objectives

- Equip participants with the skills to adjust privacy settings and protect personal data.

Content/ Method

- Teach how to adjust privacy settings on social media platforms to protect personal information.

Material

- Presentation slides explaining privacy settings for common platforms.
- Step-by-step printed guides on adjusting privacy settings for Facebook, Instagram, and Twitter.
- A projector and laptop for live demonstrations of privacy settings.

Activity 2: Adjusting Privacy Settings
Duration *20'*

Learning Objectives

- Guide participants in practicing how to configure privacy settings on social media platforms.

Content/ Method

- Interactive exercise where participants adjust privacy settings on their own social media accounts.

Material

- Computers, tablets, or smartphones for hands-on practice.
- Pre-created dummy accounts (optional) for participants without personal accounts.
- Printed worksheets with space to note privacy adjustments made.

Break | Duration *5'*

- **Provide time to rest and prepare for the next session.**
- **A short break to refresh.**

5th Session

Lecture 3: Recognizing Scams and Online Threats on Social Media
Duration *30'*

Learning Objectives

- Help participants recognize social media-specific scams and threats.

Content/ Method

- Discuss common social media scams, including phishing, fraudulent ads, fake profiles, and identity theft.

Material

- Presentation slides showcasing examples of scams, such as phishing emails and fake friend requests.
- Printed handouts detailing common scams and red flags to watch for.
- A projector and laptop for showing examples or videos of social media scams.

Activity 3: Scam Recognition Exercise
Duration *20'*

Learning Objectives

- Develop the ability to spot social media scams and learn how to avoid falling for fraudulent schemes.

Content/ Method

- Group activity where participants identify and discuss examples of social media scams, such as fake friend requests or phishing messages.

Material

- Scenario cards with examples of scams for group discussion.
- Flip chart or whiteboard to note group findings.
- Markers for capturing participant responses.

Break | Duration 5'

- **Provide time to rest and prepare.**
- **Short break to refresh.**

6th Session

Lecture 4: Engaging Safely and Responsibly on Social Media
Duration *30'*

Learning Objectives

- Explain the importance of safe and responsible social media use
- Teach learners how to develop safe sharing habits.

Content/ Method

- Presentation of "*Why is online safety important for individuals and professionals?*"**.** Examples of potential risks from unsafe sharing practices (e.g., identity theft, reputational damage). Provide learners with hypothetical scenarios (e.g., sharing vacation plans or professional achievements). Ask: *"What would you share? How would you share it safely?".* Group discussion on responses.

Material

- Slides with statistics on online risks.
- Infographic summarizing key risks and consequences of unsafe practices.

Activity 4: Reviewing Past Posts and Information
Duration *20'*

Learning Objectives

- Enable learners to evaluate and modify their social media profiles and posts for safety.

Content/ Method

- Guided audit of a sample social media profile (fictional or anonymized example). Identify unsafe or overly personal content (e.g., phone numbers, locations, sensitive photos). Demonstrate how to delete or modify posts and adjust privacy settings.

Material

- Example social media profile (printed or on-screen).
- Step-by-step guide for adjusting privacy settings (PDF or handout).

7th Session

Discussion | Duration *10'*

Learning Objectives

- Encourage a proactive mindset in recognizing and reporting suspicious activity on social media.

Content/ Method

- Group discussion on how to handle suspicious social media activity, such as how to report scams and recognize fake accounts.

Material

- Whiteboard and markers for brainstorming ways to report scams and handle suspicious accounts.
- Printed resources with contact details for reporting scams (e.g., links to platform help centers

Wrap-Up | Duration *5'*

Learning Objectives

- Summarize the training and ensure participants understand how to protect themselves from social media threats.

Content/ Method

- Review key points on social media scams and threats, answer lingering questions, and provide resources for continued learning.

Material

- Handouts summarizing key points covered in the session: ***Social media safety checklist***

5.4 Additional Information

5.4.1 Trainers' Self Reflection

- Did I effectively communicate the importance of online safety and social media engagement?
- Did I ensure that participants understood the technical aspects of privacy settings and scam recognition?
- How did I engage the participants in the activities and discussions?
- Were the resources and materials helpful to the participants?

5.4.2 Trainers' Evaluation of the Program

- Is the content of the training relevant and clear for seniors?
- Were the activities and discussions effective in helping participants learn the material?
- Do the outcomes align with the module's learning objectives?

5.4.3 Materials, Additional Resources

Appendix 1 | Icebreaker Activity: Social media Bingo

Social Media Bingo Card – A

Like	Comment	Facebook	Story	Hashtag
Selfie	Message	Instagram	Tag	Profile
Emoji	Follower	FREE	Tweet	Share
Video	Privacy	LinkedIn	Status	Post
Timeline	Notification	Twitter	Group	Reels

Social Media Bingo Card – B

Tag	Post	Instagram	Story	Privacy
Message	Facebook	Timeline	Like	Group
Reels	Hashtag	FREE	Status	Comment
Tweet	Share	LinkedIn	Video	Selfie
Follower	Notification	Profile	Emoji	Block

Social Media Bingo Card – C

Status	Like	LinkedIn	Selfie	Share
Facebook	Emoji	Instagram	Tweet	Reels
Message	Privacy	FREE	Group	Story
Timeline	Tag	Notification	Post	Hashtag
Block	Follower	Video	Comment	Profile

Appendix 2 I Lecture 1: Overview of social media

Slides to present:

- **Facebook:** "This is the most widely used platform for staying in touch with friends and family. You can share photos, comment on updates, join interest groups, and more."
- **Instagram:** "This platform focuses on pictures and videos. It's great for sharing moments visually, using features like 'Stories' that disappear after 24 hours."
- **LinkedIn:** "Think of this as your professional CV online. It's useful for job searching and networking, though not commonly used among seniors unless they're still active in the workforce."
- **Twitter:** "Here, users post short text messages called tweets. It's used mostly for following news and public figures."

Social Media Platforms Comparison

Category	Facebook	Instagram	LinkedIn	Twitter	Twitter (duplicate column)
Purpose	Connecting with friends & family	Sharing photos & short videos	Professional networking	Sharing short updates	Sharing short updates
Post Types	Text, photos, videos, links, stories	Photos, videos, reels, stories	Job updates, articles, resumes	Tweets (text), photos, videos	Public, followers
Comments & Reactions	Friends, groups, public	Followers, public	Professional contacts	Likes, comments	Likes, comments
Messaging	Messenger app	Likes, comments	Likes, comments	Likes, comments, retweets	Likes, retweets
Privacy Settings	Customizable: public, friends, groups	Limited, mostly public unless private	More public-facing by default	Mostly public, limited control	Public name & posts by default
Profile Visibility	Adjustable: name, photos, bio	Limited control unless private account	Public unless adjusted by default	Public name & adjusted	Public name & posts by default
Common Risks	Fake accounts, oversharing, scams	Scams in DMs, impersonation	Phishing messages, impersonation	Harassment, fake links, impersonation	Harassment, fake links, impersonation
Good For	✓	✓	✓	✓	✓

Appendix 3 | Activity 1: Platform Familiarization

Trainer guides group step-by-step:

"Open your internet browser and go to www.facebook.com or www.instagram.com."
"Click on 'Create new account' and fill in your information — name, birthday, etc."
"When you're asked to choose a password, make sure it's strong. A good password has at least 8 characters, uses a mix of letters and numbers, and includes a symbol."

Trainer adds:

"For example, instead of 'maria123', you could use 'Maria!74books'."
"Now let's enable two-factor authentication — Two-Factor Authentication (2FA) adds an extra layer of security. After entering your password, you will be asked for a code sent to your mobile phone or email.''

Appendix 4 | Account Setup Checklist, Account Setup Checklist

1. Choose a platform (Facebook, Instagram, etc.)
2. Go to the official website or download the official app.
3. Click on 'Create new account'.
4. Enter your real name and date of birth.
5. Use a strong and unique password (see Handout 2).
6. Provide your mobile phone or email address.
7. Enable two-factor authentication.
8. Skip unnecessary personal information (like your address).
9. Review your privacy settings right after creating the account.
10. Log out when using a public or shared device.

Account Setup Checklist

A strong password should:

- Be at least 8 characters long.
- Include a mix of uppercase and lowercase letters.
- Include at least one number and one special character (e.g., !, @, #, $).
- Avoid using common words or easily guessable information (like your name or birthday).
- Be unique for each account you create.

Example of a weak password: maria123
Example of a strong password: M@r!a74Books

Appendix 5 | Lecture 2: Privacy Settings

Social Media Privacy Checklist

[ ] Have you reviewed your profile visibility settings?

[ ] Are your posts limited to 'Friends' or 'Followers' only?

[ ] Have you enabled two-factor authentication on all platforms?

[ ] Do you avoid sharing your phone number, home address, or full birthday?

[ ] Have you checked who can send you messages or friend requests?

[ ] Do you review tagged photos and posts before they appear on your profile?

[ ] Are you cautious when accepting new friend or follower requests?

[ ] Have you deleted old posts that contain sensitive information?

[ ] Do you regularly check your privacy settings?

[ ] Are you aware of where to report scams and abuse on each platform?

Privacy Settings Guide

Links and steps to adjust your privacy settings on popular platforms:

1. Facebook:

- Go to Privacy Checkup Tool: https://www.facebook.com/privacy/checkup
- Privacy Center: https://www.facebook.com/privacy/center
- Adjust who can see your posts, who can send you friend requests, and who can look you up.

2. Instagram:

- Go to Safety Center: https://help.instagram.com/196883487377501
- How to Set Your Instagram Account to Private: https://help.instagram.com/448523408565555
- Set your account to private, manage comments, and control tags.

3. LinkedIn:

- Go to Privacy Settings Overview: https://www.linkedin.com/help/linkedin/answer/66
- Manage Your LinkedIn Public Profile Settings: https://www.linkedin.com/help/linkedin/answer/83
- Choose who can see your connections, profile details, and activity.

4.Twitter (X):

- Go to Safety Settings: https://help.twitter.com/en/safety-and-security/twitter-privacy-settings
- Security and Account Access: https://help.twitter.com/en/managing-your-account/accessing-your-twitter-data
- Protect your tweets, limit who can message or mention you, and control discoverability.

Appendix 6 | Activity 2: Adjusting Privacy Settings

Privacy Adjustment Worksheet

Use this worksheet to track the changes you make to your social media privacy settings. After reviewing your account, please indicate below the details of the changes you have made and the reasons for them.

1.

Setting Adjusted _____

New Value/Option _____

Reason for Change _____

2.

Setting Adjusted _____

New Value/Option _____

Reason for Change _____

3.

Setting Adjusted _____

New Value/Option _____

Reason for Change _____

4.

Setting Adjusted _____

New Value/Option _____

Reason for Change _____

5.

Setting Adjusted _____

New Value/Option _____

Reason for Change _____

Appendix 7| Lecture 3: Recognizing Scams and Online Threats on social media

Key takeaways of the most common scams:

- **Phishing:** *"These are fake messages that try to trick you into giving your personal information. For example, a message saying, 'You won a prize! Click here to claim it'."*
- **Fake Friend Requests:** *"You might receive a request from someone pretending to be your cousin or neighbor — always double-check."*
- **Suspicious Links:** "*These can infect your device or steal your passwords. If the link looks odd or you weren't expecting it — don't click."*
- **Impersonation and Romance Scams:** *"Some people may start a friendship or romantic conversation just to ask for money later."*
- **Fake Identities***: "Scammers create fake profiles online to build trust and manipulate victims into giving up money or personal details."*

Appendix 8| Scam Recognition Guide

Learn how to identify common scams on social media:

1. Phishing Messages:

- Look for urgent requests like "Your account will be locked!"
- Check the sender's email or username — does it look suspicious?

2. Fake Friend Requests:

- Be cautious of people you don't know.
- Watch for duplicate profiles pretending to be someone you know.

3. Prize or Lottery Scams:

- "You've won!" messages are almost always scams.
- Never provide your banking details or pay to claim a prize.

4. Romance or Friendship Scams:

- Scammers may build trust, then ask for money.
- Be cautious if someone gets too personal too fast.

5. Suspicious Links:

- Don't click on unknown links, especially those sent in private messages.
- Always double-check and report suspicious activity

Appendix 9| Social Media Safety Tips

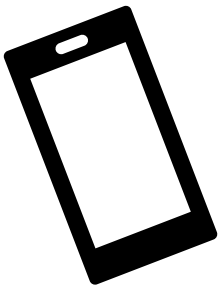
Follow these essential tips to stay safe on social media:

- Set your profile to private and control who can see your posts.
- Use strong, unique passwords for every account.
- Turn on two-factor authentication for extra security.
- Don't accept friend requests from strangers.
- Be mindful of what you post – avoid sharing travel plans or personal info.
- Log out when using public or shared devices.
- Report anything suspicious, including scams and fake accounts.
- Keep your apps updated to stay protected from new threats.
- Think before you click on links or download files.
- If in doubt, ask someone you trust or report the issue.

Stay informed. Stay safe.

Appendix 10 |Activity 3: Scam Recognition Exercise

Scenario 1: You've Won!



You receive a message from an unknown account saying:
"Congratulations! You've won a new smartphone! Click the link below to claim your prize."
The message includes a link and asks you to enter your personal information.

Scenario 2: Friend in Trouble

You get a message on Facebook Messenger from a friend you haven't spoken to in a while. They say they are stuck abroad and need you to send them 500 EUR immediately.

They ask for your phone number and bank details.

Scenario 3: Bank Alert

An account claiming to be your bank sends a direct message on Instagram:
"We have detected suspicious activity on your account. Please confirm your login details immediately by replying here."
The account profile has a bank logo as its picture.

Scenario 4: Job Opportunity

You receive a connection request on LinkedIn from someone claiming to be a recruiter. They offer you a remote job with high salary and flexible hours.
After you accept, they ask for your resume, ID photo, and your social security number.

Scenario 5: Local Community Group

You are invited to join a Facebook group for local seniors. The group shares health tips, event updates, and community news. Members are friendly and no one asks for personal data.

Appendix 11 | Lecture 4: Engaging Safely and Responsibly on social media

Safe Sharing Guidelines

Use the following guidelines to share responsibly on social media:

- Think before you post: Would you be okay if a stranger saw this?
- Avoid sharing your exact location, especially in real-time.
- Don't announce long trips or when your house will be empty.
- Never post personal documents like IDs, tickets, or bank info.
- Be cautious about sharing children's photos – get permission when needed.
- Use privacy settings to control who sees your posts.
- Avoid sharing sensitive topics in public posts.
- Don't share content when emotional – pause and reflect first.
- Use private messages for personal conversations instead of public comments.
- Regularly review your past posts and delete anything that feels unsafe.

Remember: Once something is online, it's hard to take it back.

Appendix 12 | Activity 4: Reviewing Past Posts and Information

The trainer says:
"Now we'll go into your social media accounts and look at past posts or photos. This is called a 'Digital Housekeeping' exercise."

Trainer guides the steps:

- *"Go to your profile or timeline."*
- *"Review 3–5 older posts. Ask yourself: Is this something I'd share today? Does it reveal private info?"*
- *"If yes — let's delete or edit it. I'll show you how."*

Trainer demonstrates on screen or projector:

- *How to delete a Facebook post*
- *How to untag yourself from photos*
- *How to change visibility from "Public" to "Friends"*

Appendix 13 | Profile Safety Checklist

Use this checklist to review the safety of your social media profile:

[ ] Is your profile picture appropriate and non-identifying (no personal details like home address in the background)?

[ ] Have you removed or hidden your birthdate, phone number, or home address from your profile?

[ ] Are your posts set to 'Friends Only' or 'Private' rather than 'Public'?

[ ] Have you reviewed who can comment on or share your posts?

[ ] Have you checked who can send you friend/follow requests?

[ ] Are you using a strong, unique password for your account?

[ ] Is two-factor authentication enabled?

[ ] Do you regularly review posts and delete anything outdated or unsafe?

[ ] Have you turned off location sharing in your posts?

[ ] Are you reviewing posts you're tagged in before they appear on your timeline?

Complete this checklist every few months to keep your profile secure.

Appendix 14 | Social Media Safety Checklist

[ ] Use strong, unique passwords for each account

[ ] Enable two-factor authentication

[ ] Review and adjust privacy settings regularly

[ ] Be mindful of the personal information you share publicly

[ ] Think before accepting friend or follow requests

[ ] Watch out for scams, phishing, and suspicious messages

[ ] Be cautious when clicking on links or downloading content

[ ] Report and block suspicious or abusive users

[ ] Limit location sharing and geotagging

[ ] Keep your apps and devices updated

Appendix 15| Recommendations for further reading and learning for participants

Cybersecurity websites: European and governmental organizations dealing with cybersecurity

1) **ENISA (European Union Agency for Cybersecurity)**

   Website: https://www.enisa.europa.eu/

   ENISA is the EU agency responsible for cybersecurity. It publishes reports, guides, and alerts on cyber threats and provides practical advice for citizens and organizations.

2) **CERT-EU (Computer Emergency Response Team for the EU Institutions)**

   Website: https://cert.europa.eu/

   CERT-EU monitors cyber threats and responds to cyberattacks targeting European institutions. It also offers alerts and best practices that can be applied by trainers and end users.

3) **EC3 – Europol Cybercrime Centre**

   Website: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

   Europol's EC3 provides information on online fraud, scams, and other forms of cybercrime. It publishes awareness materials and case studies relevant for identifying risks on social media.

4) **Stay Safe Online – National Cybersecurity Alliance (USA)**

   Website: https://staysafeonline.org/

   A resource hub with simple checklists and campaigns on privacy, password safety, phishing, and social media awareness.

5) **AARP Fraud Watch Network**

   Website: https://www.aarp.org/money/scams-fraud/

   An accessible US-based initiative with up-to-date information on scams that particularly target older adults, offering prevention tips and reporting advice.

6) NCSC UK – Social Media Guidance

   Website: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/social-media

7) NCSC UK – Password Guidance

   Website: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/passwords

8) LinkedIn Help – Privacy Settings

   Website: https://www.linkedin.com/help/linkedin/answer/66

5.5 Module IV – Pre/Post Test

1. What does “personal data” include?

A) Only your social media posts
B) Any information that can identify you, such as your name or ID number
C) Only your bank account details
D) Only your online passwords

2. Why is it important to read privacy policies?

A) They contain jokes about data security
B) They explain how your data will be collected and used
C) They help your device run faster
D) They are legally required but unimportant

3. Which of the following is an example of sensitive personal data?

A) Favorite color
B) Home address
C) Medical history or biometric data
D) Shopping preferences

4. What is the best practice when sharing photos or information online?

A) Share all personal details to be open and social
B) Check who can see the information before posting
C) Post frequently to stay visible
D) Always include your location

5. What does “data encryption” mean?

A) Hiding files in a secret folder
B) Changing information into a code to protect it from unauthorized access
C) Saving your files on a flash drive
D) Deleting all old data

6. Why should you limit the amount of information shared on social media?

A) It saves internet data
B) It reduces the risk of identity theft and fraud
C) It increases the number of followers
D) It prevents others from commenting

7. What should you do before granting an app access to your personal information?

A) Accept immediately to use the app faster
B) Read the permissions carefully and only allow necessary ones
C) Allow all permissions to avoid app errors
D) Uninstall the app right away

8. What is the purpose of the General Data Protection Regulation (GDPR)?

A) To help companies collect more data
B) To protect individuals' personal data and privacy rights
C) To prevent people from using social media
D) To control online shopping activities

9. Which of the following actions helps protect your data on a shared computer?

A) Staying logged in for convenience
B) Logging out and clearing browser history after use
C) Allowing browsers to save your passwords
D) Sharing your login details with family members

10. What should you do if you suspect your personal data has been stolen?

A) Ignore it and hope it resolves itself
B) Post about it on social media
C) Report it to the relevant authorities and change passwords immediately
D) Do nothing unless money is stolen

Answer Key Summary

1	**B**
2	**B**
3	**C**
4	**B**
5	**B**
6	**B**
7	**B**
8	**B**
9	**B**
10	**C**

MODULE V

Safe Digitalization of Seniors

6. Module V - Safe Digitalization of Seniors

Module 5 focuses on equipping educators with the knowledge, tools, and working methods needed to effectively support seniors in the safe use of digital technologies. The module introduces participants to the specific characteristics and learning needs of older adults, particularly in relation to using internet applications, e-mail services, social media platforms, and online banking tools.

A strong emphasis is placed on cybersecurity, with particular attention given to minimizing the risks of fraud, scams, and disinformation. Participants explore common online threats faced by seniors and learn how to address these risks through preventive strategies, clear communication, and practical guidance tailored to this age group.

In addition, Module 5 provides comprehensive educational support for senior digitalization by combining teaching tools with hands-on exercises. Participants develop skills to transfer knowledge effectively and empathetically, respond to cybersecurity-related challenges, and design accessible and supportive learning environments for both individual coaching sessions and group-based training activities.

6.1 Learning Objectives

The aim of this module is to enable participants to acquire the educational and practical skills necessary to effectively teach seniors how to safely use digital technologies and support them in coping with the challenges of cybersecurity.

- Understanding the specific needs of seniors in terms of digitalization.
- Learning teaching methods tailored to seniors.
- Gaining the skills to identify and respond to typical cyber threats aimed at seniors.

6.2 Structure, Content & Learning Outcomes

On successful completion of this module, learners will be able to:

- Understanding the barriers to learning technology by seniors (psychological, cognitive and technical), using practical and accessible teaching methods such as repetition, exercises in small steps and simple explanations.
- Learn methods for communicating the rules of safe login, recognizing safe sites and protecting personal data, supporting seniors in independent and safe use of online services.
- Become familiar with the most common threats to which seniors are particularly vulnerable and will learn how to convey this knowledge in a simple way to build seniors' vigilance.
- Learn how to support seniors in recognizing online threats and developing safe habits through exercises and situational scenarios.
- Knowing what actions to take in a threat situation, such as immediately changing passwords or disconnecting a device from the network, understanding what data is key to protecting in a threat situation.
- Knowing the procedures for reporting cyberthreat incidents, such as contacting your bank, the police or specialist organizations, what sources of support exist for victims of cybercrime
- Explaining the methods of safety rules in instant messaging, emails and video call applications and how to conduct exercises on recognizing online threats.
- Providing knowledge on protecting devices from viruses and step-by-step learning to update systems in an accessible and understandable way.

6.3 Agenda I Detailed Session Plan

MODULE V
Safe digitalization of seniors

1st Session

Welcome
Duration *5'*

Learning Objectives

- Creating an open and engaging atmosphere that encourages active participation.

Content/ Method

- Welcome of participants, short presentation of the trainer. The trainer presents the training plan and work rules.

Material

No additional materials.

Comments

It may be helpful to explain the goal of the workshop in simple language.

2nd Session

Icebreaker Activity
Duration *15'*

Learning Objectives

- Building a friendly relationship between participants, getting to know each other and activating the group before the substantive part begins.

Content/ Method

- A short activating exercise that initiates a discussion: "What challenges do they encounter when teaching seniors new technologies? How do they deal with them?" The trainer can add supporting questions that will influence the development of the discussion: What was surprising to you? What methods proved to be the most effective? How can the pace or form of classes be adjusted to the individual needs of the participants? Each participant can present one challenge.

Material

No additional materials.

Comments

It's useful to write participants' answers on a whiteboard or flipchart to identify the most common difficulties.

3rd Session

Lecture 1: Practical tips on how to teach seniors about cyber security and new technologies
Duration *25'*

Learning Objectives

- Raising awareness among educators about the barriers seniors face when learning to use new technologies, and equipping them with effective teaching tools to support the learning process.
- Providing educators with knowledge and methods for teaching seniors the principles of safe use of internet applications, strengthening their sense of security and digital competences.

Content/ Method

- The lecture is divided into two thematic areas:

Topic 1: Methods of effective teaching of seniors in the field of cybersecurity and new technologies
Content / Methods:

- Identification of psychological barriers (e.g. fear of technology, low self-confidence), cognitive barriers (e.g. slower processing of information, difficulty concentrating) and technical barriers (lack of experience with devices).
- Discussion of the principles of friendly communication with seniors.

Material:
Teaching aid for educators: Practical methods of teaching seniors – exercise material for educators (Appendix 1)

Topic 2: Preparing educators to teach seniors the principles of safe use of internet applications (banking, shopping, social networking sites)
Content / Methods:

- Review of popular internet applications used by seniors.
- Learning to recognize secure websites and applications (certificates, URLs, appearance of login forms).
- Discussion of the principles of creating secure passwords and storing login data.
- Practical exercises on fictitious accounts: logging in, checking the security of the site, simulated online shopping.

Material:
Teaching aid for educators: Practical exercises – teaching educators the principles of cybersecurity for seniors (Appendix 2)

Comments
It's useful to write participants' answers on a whiteboard or flipchart to identify the most common difficulties.

Activity 1: Identifying barriers to learning among older people
Duration *15'*

Learning Objectives

- Increasing awareness of the learning process of older people.
- Recognizing barriers to learning among seniors.

Content/ Method

- The exercise is carried out individually or in pairs – depending on the preferences of the participants.
- Participants receive worksheets (Appendix 3), which contain a task consisting of reflecting on possible barriers in the learning process of seniors.
- Participants are to identify examples of psychological, cognitive, technical barriers that may appear in seniors during their learning.
- Then they propose ways to overcome each of these barriers and describe how they may affect the learning process of seniors.
- The exercise ends with a discussion moderated by the leader, during which participants share their conclusions and experiences.

Material

- Worksheet – Identifying Barriers in Senior Learning (Appendix 3)

Comments

It is worth encouraging participants to actively participate in the discussion.

Break | Duration *5'*

- **Allow time for participants to recharge and reflect.**
- **Short break to refresh.**

4th Session

Lecture 2: Introduction to cybersecurity for seniors
Duration *35'*

Learning Objectives

- Familiarization with the most common threats to which seniors are particularly vulnerable, and learning how to convey this knowledge in an accessible and effective way to build seniors' vigilance and increase their safety on the Internet.
- Gaining knowledge on how to support seniors in recognizing online threats and how to shape habits of safe use of the Internet in them, thus increasing their digital awareness.

Content/ Method

- The lecture is divided into two thematic areas:

Topic 1: Common digital threats and the needs of seniors

Content/Methods:

- Discussion of common online threats, such as phishing, online fraud, data theft, fake news.
- Identifying specific risks to which seniors are more susceptible.
- Tips on how to effectively educate seniors about these threats without causing unnecessary fear.
- Examples of online frauds that seniors may encounter and how to recognize them.

Material:

Teaching aid for educators: Safe use of the Internet by seniors (Appendix 4)

Topic 2: Building digital awareness among seniors

Content/Methods:

- Discussion of methods for supporting seniors in learning to recognize suspicious situations on the Internet.
- Examples of exercises that help seniors remember the principles of cybersecurity.
- Simulations of online situations in which seniors may make mistakes and how to effectively help them learn to avoid these mistakes.

Material:

Teaching aid for educators: Recognizing threats on the Internet (Appendix 5)

Comments

Encourage participants to share experiences from working with seniors and examples of effective methods for explaining difficult topics.

Activity 2: Simulation exercise: talking to a senior about cybersecurity

Duration *15'*

Learning Objectives

- ❖ Allowing the educator to talk to the senior, helping them understand how to avoid online threats.

Content/ Method

- The task is carried out in pairs, in which participants alternate between the roles of an educator and a senior citizen. The aim of the exercise is to conduct a simulated educational conversation about threats on the Internet, taking into account real situations that seniors may encounter. Each pair receives a description presenting a specific threat (Appendix 6).
- The role of the educator consists of a calm, understandable explanation of what a given threat is, how to recognize it and how to react. The role of the senior citizen allows you to take on the role of a person who may have limited digital knowledge and needs clear, friendly instructions. The exercise ends with a joint discussion moderated by the leader, during which participants share their feelings, conclusions and reflections on effective educational communication with seniors.

Material

- Simulation Exercise: Talking to a Senior about Cybersecurity (Appendix 6)

Comments

It is worth paying attention to the clarity of the language and avoiding technical jargon.

Break | Duration *5'*

- **Provide time to rest and prepare for the next session.**
- **A short break to refresh.**

5th Session

Lecture 3: Responding to cyber threats

Duration *30'*

Learning Objectives

- Preparing educators to effectively provide seniors with knowledge about digital threats and how to avoid them.
- Developing the skills of educators in conducting classes with seniors on responding to cyber threats.
- Strengthening the competences of educators in the use of activation methods and methods tailored to the needs of older people.

Content/ Method

- The lecture is divided into two thematic areas:

Topic 1: Steps to take in the event of a suspected cyber attack

Content/Methods:

The trainer discusses:

- the most common symptoms of a potential cyber-attack (e.g. strange device behavior, suspicious emails, error messages, sudden log-outs);
- basic security rules - how to react in the event of a suspected attack: immediate disconnection from the network, changing passwords, not opening suspicious attachments or links;
- the importance of staying calm and not taking rash actions (e.g. not calling back unknown numbers, not clicking on phishing warnings);
- ways to create secure passwords and update them - including avoiding birthdays and simple combinations.

Topic 2: How to report digital threats and where to seek help

Content/Methods:

The trainer discusses:

- institutions and places where you can report cyber threats (e.g. CERT Polska, bank hotlines, local police, organizations supporting seniors);
- when and how to contact the bank - e.g. when you suspect an account takeover, an unauthorized transaction;

- how to prepare for reporting - writing down the date, time, content of the message, taking a screenshot, saving suspicious messages;
- the role of emotional and informational support - how and where to look for it (hotlines, advisory points, loved ones);
- the importance of reporting attempted fraud, even if no losses have occurred - for the good of other users.

Material

- Teaching aid for educators: Scenario simulations (Appendix 7)

Comments

It is worth encouraging participants to engage in discussion.

Activity 3: Scam Recognition Exercise
Duration *20*'

Learning Objectives

- Gaining knowledge on how to help seniors stay calm and composed in online threat situations (e.g. attempted fraud, suspicious emails, unknown phone calls).
- Developing the ability to make rational decisions, avoid hasty actions and contact the right people and institutions.

Content/ Method

- The exercise consists of conducting a simulation of a conversation between a senior and an educator.
- Participants work in pairs, playing the assigned roles: educator and senior. Participants have access to tips and simulation topics (Appendix 8), which help them conduct a realistic conversation about cyber threats. After the simulation ends, the leader moderates the discussion. Each pair shares their reflections with the group, discussing the difficulties they have encountered, emotions, and effective communication strategies. The discussion helps to better understand the methods of supporting seniors in recognizing threats and learning how to respond to them appropriately.

Material

- Simulation Exercise: Sample Cyber Threat Reports (Appendix 8)

Comments

It is important that educators are well prepared to engage seniors and motivate them to actively participate in learning, using examples from their everyday lives.

Break | Duration 5'

- **Provide time to rest and prepare.**
- **Short break to refresh.**
- **Short break for refreshment and relaxation.**

6th Session

Lecture 4: Educating seniors on how to use electronic devices and internet applications – a guide for educators

Duration *20'*

Learning Objectives

- Equipping educators with tools and methods that enable effective teaching of seniors the principles of safe use of communication applications such as e-mail, instant messaging (e.g. Messenger, WhatsApp) and video call applications (e.g. Zoom).
- Preparing educators to conduct classes on the protection of seniors' digital devices - from basic use of antivirus programs to learning how to update the operating system and applications.

Content/ Method

- The lecture is divided into two thematic areas:

Topic 1: How to teach seniors to use communication applications safely

Content / methods:

- Ways to explain basic functions of communication applications in simple, everyday language.
- Examples of exercises supporting the recognition of dangerous messages (spam, phishing), e.g. analysis of real and fake e-mails.
- Practical demonstrations of privacy and security settings in applications - blocking unknown contacts, changing passwords, privacy settings.
- Activation methods: working with a checklist, simulations of dangerous situations, joint solving of scenes.

Material:

Teaching aid for educators: How to teach seniors to safely use communication applications (Appendix 9)

Topic 2: How to teach seniors to use antiviruses and system updates

Content / methods:

- How to explain to seniors in an accessible way the concepts of: computer virus, update, system scanning.
- Group exercises on the installation and use of free antivirus programs (e.g. Avast, AVG).
- Step by step: how to show seniors how to perform system and application updates.

Material:

Teaching aid for educators: How to teach seniors to use antiviruses and system updates (Appendix 10)

Comments

During the discussion, it is important to ensure an exchange of ideas between participants.

Activity 4: Practical advice and techniques for seniors
Duration *30'*

Learning Objectives

- Developing the ability to provide seniors with simple and effective advice on how to use the Internet safely.
- Developing the ability to recognize and apply teaching techniques that are understandable and accessible to seniors.
- Sharing good practices and real experiences from working with seniors that can be an inspiration for other educators.

Content/ Method

- The exercise consists of two stages of work: individual and group. In the first stage, participants fill out the worksheet (Appendix 11) independently, writing down their own reflections, observations and ideas regarding effective methods of teaching seniors about cybersecurity. In the second stage, participants share their thoughts on the forum of the entire group, which facilitates the exchange of experiences and the search for inspiring solutions and proven practices. A joint conversation allows for supplementing knowledge, enriching perspectives and noticing different styles of educational work with seniors. At the end of the exercise, the leader initiates a discussion aimed at deepening the topic

Material

- Worksheet: Safe Internet Use: Practical Tips and Techniques for Seniors (Appendix 11)

Comments

It is worth encouraging participants to ask questions while performing the exercise.

7th Session

Discussion | Duration *10'*

Learning Objectives

- Allowing participants to share experiences and observations after the session.
- Identifying challenges related to teaching seniors.
- Initiating a collective brainstorming session to improve work with senior groups.

Content/ Method

- The trainer starts an open discussion with questions like: "What was the most difficult part?", "Which areas require further development?", "How can teaching seniors be simplified?" Participants share their reflections, practices, and conclusions from the session. Conclusions are written on a flipchart or whiteboard, making it easier to summarize and potentially use in the future.

Material

- Flipchart or whiteboard
- Markers

Wrap-Up | Duration *5*'

Learning Objectives

- Summarizing key information, answering last questions from participants, and pointing out resources for further learning.

Content/ Method

- A brief reminder of the most important topics covered during the training.
- Indicating additional sources of knowledge (e.g., educational websites, video materials).
- Thanking participants for their involvement and closing the session.

Material

- Teaching aid for educators: Websites on safe use of technology (Appendix 12).

Comments

At the end, it's a good idea to conduct a short evaluation survey.

6.4 Additional Information

6.4.1 Trainers' Self Reflection

- What was the most difficult thing for participants to understand about cybersecurity?
- What methods were most effective during the training?
- What changes could improve the participants' experience during the exercise?
- Did participants feel comfortable sharing their experiences and concerns about senior learning?

6.4.2 Trainers' Evaluation of the Program

- Were the training objectives achieved?
- What topics require expansion or modification in the future?
- What didactic techniques were most effective with this group of participants?

6.4.3 Materials, Additional Resources

Appendix 1 | Practical Methods of Teaching Seniors – Exercise Material for Educators

Complete the Educator's Exercises for each method (e.g., create guides, suggest analogies, design visuals, or describe responses).

Repetition and Step-by-Step Exercises

- **Method Description:** Short, repetitive instructions, each activity broken down into simple steps.
- **Educator's Exercise:** Develop a step-by-step instruction guide for logging into a social media platform or an online banking system (using simple and clear language).
- **Objective:** To develop the ability to formulate tasks in a logical and easy-to-follow structure.

Use of Visualizations and Real-Life Examples

- **Method Description:** Connecting abstract technological concepts with seniors' everyday experiences (e.g., comparing a password to a house key).
- **Educator's Exercise:** Suggest 3 analogies to help explain the following to seniors: password, secure website, and phishing.
- **Objective:** To help seniors understand complex concepts through references to familiar situations.

Use of Large Print Materials

- **Method Description:** Use of enlarged print, high-contrast colors, pictograms, and diagrams.
- **Educator's Exercise:** Prepare an example of a visual aid card for seniors that includes the principles of creating a secure password.
- **Objective:** To develop skills in creating materials adapted to the visual and cognitive needs of seniors.

Teaching at a Pace Adjusted to the Group

- **Method Description:** Observing participants' reactions, asking control questions, and maintaining flexibility in the pace of lessons.
- **Educator's Exercise:** Describe how you would respond if half of the group does not understand the function of an app being discussed – what steps would you take?
- **Objective:** To develop a reflective teaching approach and flexibility when working with a group with varying learning speeds.

  How to Use the Appendix:

  The annex can be used during educator workshops as a set of individual and group exercises, material for simulated senior training sessions, and a starting point for creating customized lesson plans.

Appendix 2 | Practical exercises – Teaching Educators the Principles of Cybersecurity for Seniors

Complete the practical tasks for each topic (e.g., review applications, check website security, create secure passwords, and practice with test accounts).

Content and Methods for Working with Educators:

1. Overview of Popular Online Applications Used by Seniors
   - **Educator's Task:** Familiarize yourself with the interfaces of applications such as shopping sites like Allegro, social media platforms like Facebook, and mobile banking.
   - **Method:** Analysis of screenshots, interface review on mobile devices and computers.
   - **Objective:** To recognize common elements and potential difficulties encountered by seniors.

2. Learning to Identify Secure Websites and Applications
   - **Practical Task:** Review 5 website examples – identify which are secure. Indicate the SSL certificate, URL evaluation, suspicious login forms.
   - **Method:** Comparative analysis (secure vs. insecure sites), interactive quiz.
   - **Objective:** To teach critical analysis of website security.

3. Principles of Creating Secure Passwords and Storing Login Data
   - **Exercise:** Create 3 secure passwords using the 3C rule (Complexity, Changeability, Memorability). Suggest a secure way to store login information (e.g., password managers, offline notebook).
   - **Method:** Brainstorming, discussion + mini-workshop on password creation.
   - **Objective:** To understand and convey security principles in a simple and convincing way.

4. Practical Exercises Using Fictional Accounts
   - **Task:** Log in to a test banking or online store account (simulation), make a secure "purchase," and check security elements on the site.
   - **Method:** Working in pairs with computers/tablets, situational scenarios.
   - **Objective:** To turn theoretical knowledge into practical skills that educators can pass on to seniors.

Appendix 3 | Worksheet: Identifying Barriers in Senior Learning

Fill in the worksheet by identifying barriers (psychological, cognitive, technical)

Psychological Barriers	Example	How to Solve	Impact on Learning
Fear of failure			
Lack of self-confidence			
Limited motivation			
Cognitive Barriers	Example	How to Solve	Impact on Learning
Slower memorization			
Concentration difficulties			
Short-term memory problems			
Technical barriers	Example	How to Solve	Impact on Learning
Difficulties in using technology			
Lack of experience in using the Internet			
Problems with using new educational platforms			

Appendix 4 | Safe Use of the Internet by Seniors

Present examples, discuss real-life threats, and run interactive exercises to teach seniors online safety.

1. Presentations with Examples of Online Scams

- **Description:** Presentations should include realistic examples of online scams commonly targeting seniors, such as phishing, fake auctions, or fraudulent emails. Educators can prepare slides or visual materials illustrating specific cases, showing how to recognize dangerous elements.
- **Objective:** To raise seniors' awareness of the most common online threats. To teach the recognition of scams and other forms of online abuse to which seniors may be particularly vulnerable.
- **Examples of Scams to Discuss:**
  Phishing: fake emails or websites attempting to steal login credentials.
  Online auction scams: fake product sale offers.
  Fake SMS and emails: messages pretending to be from institutions, such as banks.

2. Discussion on Real-Life Threats in Seniors' Daily Lives

- **Description:** After presenting examples of scams, it is important for the educator to lead a discussion that allows participants to share their experiences and knowledge about online threats encountered by seniors. Educators should encourage seniors to talk about their own experiences and difficulties they face when using technology.
- **Objective**: To understand the real dangers that seniors encounter in their everyday lives. To identify barriers to internet use among seniors, such as lack of digital skills or fears related to safety.
- **Sample Discussion Questions**
  - What types of online scams have you encountered or heard about?
  - What are the main online security concerns seniors have?
  - What is the biggest challenge for seniors when learning to use the internet?

3. Interactive Exercises and Simulations for Identifying Online Threats

- **Description:** Exercises and simulations help apply online safety knowledge in practice. Seniors can participate in activities where they need to identify which websites or messages are safe and which may be dangerous. Educators can use examples such as a fictional bank account, online store, or social media profile to demonstrate in real-time how to recognize suspicious elements.
- **Objective:** To enhance the ability to recognize internet threats through hands-on practice. To develop seniors' ability to make informed decisions about their online safety.
- **Sample Exercises**
  - *Phishing recognition exercise:* Participants receive sample emails and must indicate which ones might be phishing attempts.
  - *Online shopping simulation:* A group analysis of an e-commerce site, checking how to recognize fake offers and what elements indicate a website is secure
  - *Website safety assessment:* Reviewing websites and identifying suspicious elements such as missing SSL certificates or questionable login forms.

Appendix 5 | Recognizing threats on the Internet

Teach seniors to recognize online threats and practice with emails, links, and passwords.

1. Overview of methods to support seniors in recognizing suspicious online situations

- **Description**

  Educators should use a variety of methods that enable seniors to recognize suspicious situations on the internet. The main goal is to build awareness that not everything that appears trustworthy actually is. Clear and simple guidelines can help seniors independently assess whether a given situation is safe.

- **Methods**

  - Basic principles for identifying suspicious situations: Teaching seniors how to spot suspicious emails, SMS messages, or fake websites. Examples: lack of SSL certificate, spelling mistakes in messages, inconsistent URLs.
  - The "don't trust the unknown" rule: A joint discussion on situations in which seniors might receive suspicious offers (e.g., fake investment opportunities, contest winnings, or unknown requests for personal data).
  - Education through analogies: Comparing online situations to real-life scenarios, such as recognizing a shady vendor at a market.

2. Examples of exercises that help seniors remember cybersecurity rules

- **Description**

  Practical exercises that engage seniors help reinforce cybersecurity principles and cautious behavior online. Seniors are more likely to remember these rules when they have a chance to apply them in a safe and controlled environment.

- **Exercises**

  - Recognizing fake emails: Participants receive various examples of emails (authentic and fake). Their task is to identify which emails may be scams and which are safe.
  - Detecting dangerous links: Seniors practice identifying suspicious links in emails or SMS messages, learning how to verify whether a URL is trustworthy.
  - Password safety exercise: Participants create examples of strong and weak passwords. They learn the principles of creating secure passwords and how to store them safely.

3. Simulations of online situations where seniors might make mistakes — and how to help them learn to avoid these

- **Description**

  Online simulations are practical exercises that allow seniors to learn through experience how to recognize and avoid mistakes. Simulations help participants feel more confident and aware while using the internet.

- **Methods**

  - **Phishing simulation:** The educator presents a scenario in which a senior receives an email that looks like an authentic message from a bank, asking for login details. Seniors learn how not to be deceived and which elements in the email should raise suspicion.

- **Online shopping simulation:** Seniors visit websites that imitate online stores. Their task is to identify suspicious elements such as prices that are too low, lack of an SSL certificate, or strange payment methods.
- **Fake prize announcement simulation:** Educators present a situation in which a senior receives a message about winning a contest that is actually a scam. Seniors learn to recognize such scams and how to respond.

Appendix 6 | Simulation Exercise: Talking to a Senior about Cybersecurity

Conduct a role-play on phishing, scams, account security, and social media, with the educator guiding and the senior practicing.

Task Scenario

The educator and the senior engage in a conversation about online threats, learning how to recognize and avoid risky situations. Each scenario presents different common threats that seniors may encounter on the internet.

Example topics to discuss during the exercise

- Phishing (fake emails, messages)
  How can phishing be recognized in emails, SMS messages, and websites?
  What are the typical signs of fake messages and links?
- Fake prizes and contest scams
  What are common scams involving prizes and contest winnings?
  How should one respond to offers that require an upfront payment?
- Online account security
  What are good practices for securing accounts in banks, online stores, and social media?
  What makes a password secure, and why is two-factor authentication important?
- Safe use of social media
  How can fake profiles and scammers on social media be recognized?
  What information should be protected, and what should not be shared online?

Role division in the exercise (in pairs)

- **Role of the educator (simulation trainer):**
  The educator's task is to lead the conversation, helping the senior understand online threats and teaching them how to recognize them.
  The educator should use simple and clear language, patiently explain the threats, and ask questions to encourage the senior to actively participate in the conversation.
  The educator is also responsible for reminding the senior about internet safety rules and ensuring they have understood the material.
- **Role of the senior**
  The senior takes an active part in the conversation, sharing their experiences related to using the internet. They can express any doubts or concerns about online safety.
  The senior answers the educator's questions, shares their perspective, and tries to solve the presented problems related to online threats.

- **Phishing (fake emails, messages)**

How can phishing be recognized in emails, SMS messages, and websites?

What are the typical signs of fake messages and links?

- **Fake prizes and contest scams**

What are common scams involving prizes and contest winnings?

How should one respond to offers that require an upfront payment?

- **Online account security**

What are good practices for securing accounts in banks, online stores, and social media?

What makes a password secure, and why is two-factor authentication important?

- **Safe use of social media**

How can fake profiles and scammers on social media be recognized?

What information should be protected, and what should not be shared online?

Appendix 7 | Scenario Simulations

Conduct scenario simulations where seniors face scam calls, emails, or SMS. Ask how they would react, discuss emotions and safe responses, and practice calming techniques like breathing.

Exercise Content

Preparation for the exercise

Begin the session with a brief discussion about the importance of staying calm in difficult situations. Highlight that scammers often try to create panic or a sense of urgency to pressure seniors into making quick, unthinking decisions.

Threat scenario simulations

- **Scenario 1**
  A senior receives a phone call from a "bank employee" claiming that their account has been blocked and asking them to install an app. What does the senior do?
- **Scenario 2**
  A senior gets an email about winning a contest and is asked to provide personal information and click a link. What does the senior do?
- **Scenario 3**
  A senior receives an SMS with a suspicious message about needing to pay extra for a package. What does the senior do?

After each scenario:

- Ask seniors to briefly share how they would respond in such a situation.
- Ask reflective questions like
  What do you feel when you receive such messages?
  What emotions arise?
  What thoughts influence your decisions?

Then, discuss as a group what steps to take in order to remain calm:

don't panic, don't act impulsively, pause and talk to someone close, verify the information.

Emotional awareness exercise:

Ask seniors to close their eyes and recall a situation when they felt threatened online (e.g., received a suspicious email).

Ask: *What emotions did you feel at that moment? What physical signals did your body send (e.g., increased heart rate, sense of unease)?*

Encourage them to find ways to control those emotions in a threatening situation, such as using previously discussed breathing techniques.

Exercise summary:

Emphasize how important it is to pause before making any decisions when facing a potential threat. Point out that it's not always necessary to act immediately. It's wise to ask for help or consult with loved ones or professionals before taking any steps.

Tips for the educator:

- **Be patient:** Seniors may need more time to understand the threats and respond appropriately. Patiently explain each threat and provide possible solutions.
- **Adjust the pace:** Make sure all participants understand each exercise and have the opportunity to ask questions.
- **Be mindful of emotions:** Understanding how emotions affect decision-making is essential. This is why relaxation exercises and emotional recognition are important.

Practice regularly

These sessions should be repeated regularly so that seniors feel more confident and know how to respond when facing threats.

Appendix 8 | Simulation Exercise: Sample Cyber Threat Reports

Conduct role-plays with sample cyber threats; explain, identify risks, and practice safe responses.

Task Scenario

Participants work in pairs, taking on the roles of the educator and the senior.
Each pair receives a description of one of four sample cyber threat reports.
The educator's task is to conduct a calm and clear educational conversation with the senior, during which they:

- explain the nature of the threat,
- help the senior understand how to recognize danger signs,
- work together with the senior to find solutions and safe responses to the situation.

Participants may switch roles and work with a new report.

Examples of four cyber threat reports that may concern seniors

Report 1: SMS requesting additional payment for a parcel

Situation description: The senior received an SMS informing them that a package is awaiting delivery, but an additional payment of 2 EUR is required. The message included a suspicious link leading to an unknown website.

Report 2: Fake phone call from the bank

Situation description: The senior received a phone call from someone claiming to be a bank employee. The scammer claimed that the account had been blocked and suggested installing an app to protect it.

Report 3: Email about a supposed prize

Situation description: The senior received an email claiming they had won a contest. The email requested personal data and asked the senior to click on a link leading to a suspicious website.

Report 4: Facebook account takeover

Situation description: Friends of the senior received strange messages from their account, including links or requests for a loan. The senior did not send those messages, which suggests their account was taken over by a scammer.

Suggestions for educators on how to talk about threats:

- **Understanding the situation:** Use simple language and analogies to explain threats. Seniors often understand better when situations are presented in the context of everyday life (e.g., comparing cyber fraud to traditional phone scams).
- **Examples and simulations:** Regularly conduct exercises using simulated phone conversations or by analyzing examples of suspicious emails. This helps seniors respond more effectively to real threats.
- **Assistance with reporting incidents:** Help seniors report cyber threats to appropriate institutions, such as CERT Poland, banks, or the police. This can be practiced during the training session to build their confidence.
- **Emphasizing two-factor authentication:** Provide guidance on enabling two-factor authentication, which can help seniors secure their online accounts—especially when using social media.
- **Staying calm:** Educators should teach seniors to remain calm in threatening situations and to avoid impulsive actions, such as installing unknown apps or sharing personal information.
- **Education on security tools:** It's worth introducing the use of antivirus software, securing online accounts, and verifying the credibility of information sources (e.g., checking official bank phone numbers).

Appendix 9 | How to Teach Seniors to Safely Use Communication Applications

Teach safe use of apps with simple language, practice with icons, and identify spam or phishing messages.

Content Scope and Teaching Methods

1. Explaining basic functions of communication apps in everyday language

Recommendations for the Educator

- Avoid technical jargon – instead of saying "log into your account", say "type your name and password to open your mailbox."
- Instead of "privacy settings", say "where you can choose who can see you and who can message you."
- Use analogies, e.g., "a messenger is like a phone with messages and pictures."

Example Exercise

- Distribute cards with icons of popular apps (e.g., email, WhatsApp, Messenger, Zoom).
- Ask participants to describe them in their own words.
- Together, create a simple definition for each one.

Supporting Materials

- Create a printed glossary of simple terms (e.g., "message", "video call", "attachment").

2. Exercises in identifying dangerous messages (Spam, Phishing)

Recommendations for the Educator

- Always use real examples to show both safe and fake messages.
- Discuss what a suspicious email address looks like, what "click this link" means, how to spot the "grandchild abroad" scam.

Example Exercise

- Divide participants into groups and give them three printed emails:
  - A real invitation to a conversation
  - A fake email with a link to an “invoice”
  - A message with grammar mistakes and a request for personal data
- Task: Identify which messages are suspicious and why.

Supporting Materials

- Create worksheets with sample emails for analysis
- Introduce 5 key questions for every message:
  - Do I know the sender?
  - Does the message make sense?
  - Are there any mistakes?
  - Does the email address look correct?
  - Does the link seem suspicious?

3. Demonstrating privacy and security settings

Recommendations for the Educator

- Demonstrate each task step by step on a large screen or projector.
- Remember: seniors often learn by repetition – plan to complete each step together.

Example Exercise

To complete together with participants:

- Go to WhatsApp settings → "Privacy" → "Profile Photo" → select "My Contacts"
- On Messenger: demonstrate how to block a stranger

Supporting Materials

- Create illustrated step-by-step instruction cards, e.g.:
  - "How to change your password"
  - "How to set privacy"
  - "How to block a user"

4. Interactive methods – Reinforcing knowledge and responding to threats

Recommendations for the Educator:

- Simulations are effective – seniors learn best through realistic scenarios.
- Use pairs or small groups to build confidence and teamwork.

Example Exercises:

- Simulation 1: "I received a strange message from the bank" – what to do?
- Simulation 2: "I can't connect with my daughter on Zoom" – how to check the settings?
- Role-play: educator as a scammer, participant plays the senior – then switch roles.

Supporting Materials:

- Create simulation scenarios
- Role cards: educator/participant/scammer
- Take-home reminder cards with safety tips (e.g., to stick on the fridge)

Appendix 10 | How to Teach Seniors to Use Antiviruses and System Updates

Teach seniors what viruses and updates are, demonstrate antivirus use, and practice running scans and installing system updates step by step.

Content scope and teaching methods

1. Introduction – What are viruses, updates, and security features

Recommendations for the educator:

- Remember to use analogies when explaining complex topics.
- Explain what "computer viruses" are – use comparisons to a cold or infection that can attack a computer.
- Clarify that updates are like “medicine” for a computer – they help prevent failures and attacks.

Example exercise

- Ask participants the following questions:
  - Have you ever heard of a “computer virus”?
  - What comes to mind when you hear the word “update”?

2. Demonstration of antivirus software

Recommendations for the educator:

- Use a safe and intuitive program (e.g., Windows Defender, free version of Avast).
- Go through the process step by step: opening the program, checking for updates, performing a quick scan. You may demonstrate the procedure using a projector.

Example Exercise:

- Ask participants to open the antivirus software on their own devices (or on a shared laptop).
- Perform a scan together. Discuss what the results mean: “no threats found” vs. “threats detected”.

3. Learning how to update the operating system

Recommendations for the educator:

- Show how to locate update settings (e.g., in Windows: Settings → Update & Security).
- Highlight that updates usually appear automatically – the user just needs to click “Install now”.

Example exercise:

- **Each participant receives a checklist:**
  - Open “Settings”
  - Find “Windows Update”
  - Check for available updates
  - Install update if available

- **Note: If using a shared computer, the exercise can be conducted as a demonstration with commentary.**

4. Reinforcement methods – checklists, role-plays, discussions

Recommendations for the educator:

- Provide a recap of the material in the form of a game or quiz.
- Encourage participants to ask questions and share their own experiences.

-

Example exercises:

- Security checklist: The participant checks step-by-step whether their computer/smartphone is protected (passwords, updates, scans).
- Phone call simulation: The educator plays a scammer saying, “Your computer is at risk – download our program.” The senior’s task is to recognize the threat and respond, “First, I’ll check my antivirus settings.”

Support materials:

- Ready-to-use checklists: “Secure Computer – Do I Have Everything I Need?”

Appendix 11 | Worksheet: Safe Internet Use: Practical Tips and Techniques for Seniors

Fill out the worksheet by answering questions on safe shopping, device security, online privacy, and overcoming fear of technology.

Safe Online Shopping	
What elements of an online offer should be highlighted to seniors as potentially dangerous or suspicious?	
How to guide seniors through the online shopping process – how to speak, what to show and what to look for to make them feel safe?	
Device Security	
What techniques help seniors understand how to set up their devices safely?	
What applications and settings are necessary to protect seniors’ devices	
Online Privacy Protection	
What methods will you use to help seniors better understand the concept of online privacy protection, especially in the context of using communication applications such as WhatsApp?	
Overcoming Fear of Technology	
What training elements help seniors overcome fear of technology and strengthen their sense of confidence when using the internet?	
What methods of building self-confidence are worth using to make seniors feel comfortable in the world of new technologies?	

Appendix 12 | Recommendations for further reading and learning for participants

Cybersecurity websites: European and governmental organizations dealing with cybersecurity:

1) **ENISA – European Union Agency for Cybersecurity**
   Website: https://www.enisa.europa.eu
   ENISA offers guides, reports, and educational campaigns on cybersecurity. It includes educational materials for individual users, including seniors, on safely using emails, passwords, smartphones, and online banking.
2) **European Commission – Safer Internet**
   Website: https://digital-strategy.ec.europa.eu/en/policies/safer-internet
   The European Commission's program promoting safe internet use for all age groups, including seniors. The website contains informational campaigns and links to national initiatives.
3) **European Consumer Centre Network (ECC-Net)**
   Website: https://www.eccnet.eu
   A network of consumer centers in the EU, offering advice on safe online shopping, personal data protection, and avoiding internet fraud, which can be particularly helpful for seniors.
4) **Cyberprofilaktyka – Digital Prevention Program**
   Website: https://cyberprofilaktyka.pl/
   A digital prevention program that includes a section with advice for seniors on how to avoid online threats. It also features educational materials, infographics, and examples of real-life scams to help better understand digital risks.

6.5 Module V – Pre/Post Test

1. What is the main goal of Module 5?

A) To teach seniors how to use social media for fun
B) To train educators to effectively support seniors in safe digitalization
C) To improve seniors' knowledge of artificial intelligence
D) To develop seniors' programming skills

2. Which of the following is a common barrier for seniors when learning digital skills?

A) Curiosity about new technologies
B) Fear of failure or lack of self-confidence
C) Overuse of social media
D) Strong technical knowledge

3. What is one effective teaching method for seniors?

A) Using complicated jargon to sound professional
B) Conducting lessons at a fast pace
C) Breaking instructions into small, simple steps
D) Focusing only on theoretical knowledge

4. What should educators emphasize when teaching about online banking and shopping?

A) How to spend money faster
B) How to recognize safe websites and protect personal data
C) How to increase online visibility
D) How to disable antivirus software

5. Which of the following is a good example of a phishing attempt?

A) A friend sending you a known link
B) An email from your bank asking for your login and password
C) An update from a trusted software program
D) A reminder from your calendar app

6. When a senior receives a suspicious phone call from a "bank employee," what should they do first?

A) Install the suggested app immediately
B) Hang up and call their bank through the official number
C) Give their ID and account details
D) Ignore the call completely

7. What is the best way for educators to help seniors understand antivirus programs?

A) Explain using analogies, like comparing viruses to illnesses
B) Avoid technical explanations altogether
C) Skip antivirus topics because they're too advanced
D) Only show text-based explanations

8. What does "digital awareness" mean for seniors?

A) Knowing how to shop online faster
B) Understanding and recognizing online threats
C) Avoiding all use of technology
D) Learning how to design websites

9. What should an educator do if a senior does not understand an application during class?

A) Move on to the next topic
B) Repeat and simplify the explanation patiently
C) Ask another senior to teach them
D) Ignore the problem

10. What should seniors do if they suspect a cyberattack on their account?

A) Wait to see if it fixes itself
B) Report it to the bank or authorities and change passwords immediately
C) Share the news on social media
D) Delete all their accounts

Answer Key Summary

1	**B**
2	**B**
3	**C**
4	**B**
5	**B**
6	**B**
7	**A**
8	**B**
9	**B**
10	**B**

7. Evaluation Survey

The information you provide in this survey will serve as a guideline to improve the level of training you participate in, as well as the level of effectiveness and attractiveness of your next training programs.

Please complete the survey by answering it yourself, or according to the rating scale below, where 1 is the lowest rating and 5 is the highest.

I. **Workshop evaluation:**

- Training program ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Methods of conducting classes ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Atmosphere during the classes ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Usefulness of the training ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Trainer's preparation ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Selection of the training content ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- The objectives of the training were clearly specified ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1

1. **Which issues have been useful to you and that you will definitely use?**
   .....
   .....

2. **Which issues were less useful to you?**
   .....
   .....

3. **Which of the issues that were not covered in class but you think should have been included in the program and why?**
   .....
   .....

4. **Do you think there are any topics that should be added or eliminated from the training program? Explain why?**
   .....
   .....

II. **Evaluation of training materials:**

- Content ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Accessibility of information ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Legibility ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Usefulness of materials ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1

III. **Additional information:**

1. **Overall evaluation of the training** ☐ **POSITIVE** ☐ **NEGATIVE**

2. **Did the training meet your expectations and requirements - were the intended goals, outcomes, results achieved?** ☐ **YES** ☐ **NO**

3. **Do you think it was worthwhile to organize such training (and why)?**
   .....
   .....

4. **Your additional comments and observations:**
   .....
   .....

5. **How did you find out about the training?**
   .....
   .....

www.cybersafesenior.eu

Cyber-Safe-Senior

Funded by
the European Union

CYBER SAFE
SENIOR

Instytut
Nowych Technologii

iED

ILKSENOL
DERNEĞİ

SIMBIOZA
MED GENERACIJAMI

"Funded by the EU. The views and opinions expressed are those of the author(s) and do not necessarily reflect the views of the European Union or the Erasmus+ National Agency.
The European Union nor the grantor is not responsible for them."