



Co-funded by
the European Union



GenerationInfinity

**The Generation Infinity Project:
Enhancing digital skills,
competencies and safety
in European older adults and seniors!**

WP2

MODULE 6: Digital security in the digital age



 **Bluechain**



The Generation Infinity Project (2024-1-BG01-KA220-ADU-000248972) is co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor FACFA can be held responsible for them

Author	Project Partner
Harikleia Sfouni	Bluechain Research Cooperative
Sofia Vlachou	Bluechain Research Cooperative

Creative Commons License



CC BY-NC 4.0

Creative Commons Attribution-NonCommercial 4.0 International

This license requires that reusers give credit to the creator. It allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, for noncommercial purposes only.



Project Partners



Table of Contents

Module Objectives	3
<i>Estimated time</i>	<i>3</i>
Structure of the Modules	4
<i>Additional Trainer support material – Worksheets:</i>	<i>11</i>
Module Evaluation	12
Scenarios for Training	15



Project Partners



Module Objectives

At the end of this module, the trainer will be able to:

1. Explain the core principles of digital security for older adults, including phishing and scam recognition, password safety, privacy settings, personal data protection, and safe browsing, using clear and accessible examples.
2. Design and facilitate short, practical digital safety learning activities based on real-life online situations relevant to seniors, such as suspicious messages, account log-ins, online shopping, e-government use, or social media interaction.
3. Teach digital security in a way that reduces fear, builds trust, and strengthens confidence, using plain language, repetition, step-by-step guidance, and psychologically supportive communication.
4. Help older learners recognise recurring warning patterns online and respond safely and calmly when they are unsure, rather than relying on memorising technical terms or complex rules.
5. Evaluate the learning outcomes of a digital security session using simple and practical tools such as observation checklists, short practical tasks, and self-reflection sheets.

Estimated time

2-3 hours



Project Partners



Structure of the Modules

Key Topics	Detailed Contents	Teaching Methodology for the Trainer
1.1 Why Digital Security Matters in Everyday Life	Digital security as part of everyday digital participation. Why online safety matters when using email, messaging apps, online banking, shopping, healthcare portals, social media, and e-government services. Difference between ordinary online use and risky online situations. Recognising that digital security is not only technical protection, but also confidence, judgment, and safer habits.	• Short trainer input (5-7 min) introducing digital security through familiar daily examples rather than abstract terminology. • Guided discussion (5 min) where participants identify which online activities seniors in their context use most often and where they feel most vulnerable or hesitant.
1.2 Evidence-Based Focus on Seniors' Digital Safety Needs	Typical safety-related difficulties among older adults: fear of fraud, lack of confidence, uncertainty about suspicious messages, confusion with pop-ups and links, and anxiety around making irreversible mistakes. Difference between access to technology and confident, safe use of technology. The importance of pacing, repetition, visual support, and practical relevance in digital security education. Recognising that security concerns are often emotional as well as technical.	• Guided reflection activity (5-7 min) focused on the real security concerns seniors express in training contexts. • Pair discussion where trainers identify which risks create the most fear, avoidance, or

Project Partners



Key Topics	Detailed Contents	Teaching Methodology for the Trainer
		dependence on others among the seniors they work with.
1.3 Role of the Trainer in Digital Security Education	Trainer as facilitator, safety guide, and confidence-builder. Key trainer responsibilities: choosing relevant examples, creating a non-threatening learning environment, slowing down processes, explaining “why” behind safer choices, and reinforcing safe responses without shame. Importance of ethical handling of examples involving personal data, messages, and online accounts. Using simulated materials instead of real passwords, real bank details, or sensitive personal information.	• Checklist exercise (8-10 min) where trainers review what must be prepared before a digital security session: examples of privacy-safe materials. • Short reference sheet (3-5 min) on how a trainer opens a session in calm, simple language and sets a reassuring tone.
1.4 Communication, Reassurance and Trust-Building	Using plain language instead of jargon. Explaining the risk without using fear-based language. Recognising emotional barriers such as embarrassment, mistrust, panic, or self-doubt. Encouraging “not sure” as a safe and acceptable response. Using repetition, analogies, and simple “do / don’t” principles to support understanding and retention.	• Short role-play exercise (10 min) in pairs or triads where trainers practise explaining a suspicious online situation to a senior learner in simple, calm, and reassuring language. • Brief debrief (5 min) focused on which phrases increased trust



Project Partners

Key Topics	Detailed Contents	Teaching Methodology for the Trainer
		and which ones unintentionally increased fear or confusion.
2.1 Teaching Recognition of Phishing, Scams and Online Manipulation to Older Adults	Phishing emails, scam SMS messages, fake senders, fake websites, impersonation, urgency tactics, requests for passwords, codes, banking details, or personal information. Recognising common warning patterns: pressure, secrecy, emotional manipulation, unexpected contact, suspicious links, and mismatched sender details. Using categories such as safe / suspicious / not sure. Safe response steps: stop, do not click, verify, delete, report, or ask for help.	• Scenario-based learning using simulated emails, SMS messages, and pop-ups. • Guided group analysis of warning signs, followed by short peer explanation exercises using non-technical language.
2.2 Teaching Password Safety and Account Protection in Senior-Friendly Ways	Strong password principles. Risks of password reuse across services. Safer password routines and practical ways to remember stronger passwords. Introduction to two-factor authentication. Secure log-in habits and account recovery awareness. Protecting key personal accounts such as email, banking, and public service accounts.	• Step-by-step trainer demonstration (5-7 min) showing how to move from weak password habits to safer ones without overwhelming learners. • Practical exercise (10 min) where participants compare weak and stronger password examples, discuss safer routines, and prepare a short

Project Partners



Key Topics	Detailed Contents	Teaching Methodology for the Trainer
		teaching explanation for seniors. • Optional mini-activity on when and why two-factor authentication is useful.
2.3 Teaching Privacy and Personal Data Protection Through Everyday Examples	What personal data is and why it matters. Sensitive vs non-sensitive information. Risks of oversharing on social media, messaging apps, and online forms. Permissions, privacy settings, and access control in common platforms. Recognising when information should not be shared and how to explain this clearly to older learners. Protecting identity, contact details, and routine personal information in digital spaces.	• Hands-on guided exploration of privacy settings using screenshots. • Small-group task where participants review examples of shared information and decide what is safe to share, what is risky, and what should remain private. • Guided reflection on how to explain privacy in everyday language rather than legal or technical terms.
2.4 Teaching Safe Browsing and Secure Use of Everyday	Recognising secure versus suspicious websites. Checking website addresses, login pages, links, and pop-ups. Avoiding unsafe downloads and unsafe redirections.	• Practical comparison exercise using examples of legitimate and

Project Partners



Key Topics	Detailed Contents	Teaching Methodology for the Trainer
Online Services to Seniors	Risks of public or shared devices and networks. Knowing when to stop, check, or postpone an online action.	suspicious websites. • Trainer-guided browsing simulation (10-12 min) showing how to check legitimacy cues step by step. • Pair activity in which one participant explains the browsing decision out loud while the other follows, reinforcing clarity and logic.
3.1 Responding Safely to Suspicious Situations and Mistakes	What to do when something feels wrong online. How to respond after clicking a suspicious link, opening a strange message, or sharing information by mistake. The importance of pausing, not panicking, and asking for help safely. Simple response routines that can be remembered and repeated. Moving from fear-based reactions to calm, safer decisions.	• Scenario discussion(10 min) where trainers analyse common “what if” situations and decide on the safest next step. • Guided problem-solving activity focused on calm response strategies rather than blame or shame.

Project Partners



Key Topics	Detailed Contents	Teaching Methodology for the Trainer
3.2 Building Digital Confidence and Safer Habits	Confidence grows through small successes, repetition, and visible progress. Recognising that mistakes are part of learning. Creating routines that reduce cognitive load and improve safer decision-making. Encouraging seniors to trust patterns, not panic. Strengthening resilience and independence rather than dependency on others.	• Guided reflection (5 min) on how reassurance, repetition, and simple routines change learning outcomes in digital security. • Short peer exchange where trainers identify one confidence-building habit they want to integrate into future sessions.
3.3 Evaluating Learning Outcomes in Digital Security Training	Practical evaluation focus: whether the learner can recognise common risks, explain a safer choice, and respond appropriately to suspicious situations. Simple evaluation tools: observation checklist, short practical task, self-reflection sheet. Balancing knowledge assessment with confidence and behavioural change. Using evaluation in a supportive, realistic, and non-threatening way.	• Short trainer oral exercise (5 min) presenting practical and reflective evaluation options. • Mini exercise where trainers choose one practical method for assessing a short digital security session.
3.4 Trainer Reflection and Continuous	Importance of trainer reflection after each session. Using participant reactions, mistakes, and questions to improve examples, pacing, and	• Guided reflection (5 min) where trainers identify one improvement

Project Partners



Key Topics	Detailed Contents	Teaching Methodology for the Trainer
Improvement	materials. Identifying which security topics create confusion or anxiety and adjusting methodology accordingly. Building a reusable set of examples, worksheets, and explanation strategies for future sessions.	they would apply in their next digital security session. focused on practice Short plenary wrap-up call adjustments and sustainability of materials.



Project Partners



Additional Trainer support material – Worksheets:

1. PowerPoint Presentation on digital security basics for older adults
2. Pre-Session Readiness Sheet for Digital Safety Training
3. Post-Activity Review Template: Trust, Clarity and Learner Comfort
4. Workshop Flow Design Exercise for a Short Digital Safety Session
5. Assessment Planning Table: Simple Learning Check Methods
6. Trainer Guidance Notes for Common Online Safety Scenarios
7. Reflective Follow-Up Sheet for Session Improvement



Project Partners



Module Evaluation

Instructions:

Please rate the following statements based on your experience of this module.

(1 = **Strongly disagree** | 5 = **Strongly agree**)

1. Learning Objectives

The module clearly explained the most relevant digital security topics for older adults, including phishing, scam recognition, password safety, privacy, personal data protection, and safe browsing.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

2. Practical Applicability

I feel confident designing short, practical digital safety learning activities based on everyday online situations relevant to senior learners.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

3. Facilitation & Communication

The module improved my ability to teach digital security using calm, inclusive, confidence-building, and senior-friendly communication.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

4. Online Risk Awareness

I gained clearer methods for helping older adults recognise phishing, scam messages, suspicious links, and common online manipulation tactics.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

5. Passwords, Privacy and Data Protection

The module strengthened my ability to explain passwords, privacy settings, and personal data protection in a simple, practical, and accessible way.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

6. Evaluation & Quality Assurance

The evaluation tools presented in this module are simple, realistic, and useful for assessing learning outcomes in digital security training.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

7. Overall Value

Overall, this module was relevant to my professional role and provided methods I can realistically apply in my work with older adults.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5



Project Partners

8. Reflective Question

What is one concrete digital safety rule, activity, or teaching approach you plan to apply in your future work with senior learners?

(Optional)

Any additional comments or suggestions for improving the module:



Project Partners



Scenarios for Training

Section 1- Foundations of Digital Security Learning for Older Adults	
1.1 Why Digital Security Matters in Everyday Life	Theoretical part The trainer presents digital security as an everyday life skill rather than a technical subject. The focus is placed on situations that seniors already encounter, such as using email, receiving messages, shopping online, accessing public services, or using online banking. The trainer explains that digital security is closely linked to confidence, and safe routines, and not only to technical knowledge. Practical part The trainer invites participants to map common digital situations in which older adults may feel uncertain or exposed. In pairs or small groups, participants identify which daily online activities involve the highest risk and discuss how they would explain these risks to seniors in simple and reassuring language.
1.2 Evidence-Based Focus on Seniors' Digital Safety Needs	Theoretical part The trainer explains that many seniors' difficulties with digital safety are shaped by fear of fraud, uncertainty, low confidence, and previous negative experiences. The focus should therefore not be only on information, but also on emotional readiness, pacing, repetition, and practical relevance. The trainer highlights that safe digital participation depends on understanding, trust, and confidence.



Project Partners

	Practical part Participants reflect on the most common security fears they have observed among older learners, such as scams, suspicious messages, pop-ups, or accidental clicks. They then discuss how these fears affect learning behaviour and what type of trainer response can reduce hesitation and increase engagement.
1.3 Role of the Trainer in Digital Security Education	Theoretical part The trainer is presented as a facilitator of safe learning, not only as a source of information. Their role includes choosing relevant examples, slowing down the process, preventing shame, and helping seniors develop safer decision-making habits. Ethical care is also important, especially when using examples involving personal data, online accounts, or screenshots of digital interactions. Practical part Participants review a short preparation checklist for a digital security session, including examples. They then simulate the opening of a short session, focusing on how to introduce the topic calmly, explain the objectives clearly, and create a respectful atmosphere from the beginning.
1.4 Communication, Reassurance and Trust-Building	Theoretical part The trainer explains that communication style strongly influences whether seniors feel safe enough to learn. Plain language, visible pacing, repetition, and calm reassurance are essential. It is equally important to avoid jargon, fear-based language, and behaviours that make

Project Partners



	learners feel rushed, judged, or dependent. Practical part In pairs or triads, participants role-play a short trainer-senior interaction involving a suspicious online situation. The objective is to practise calm explanation, supportive phrasing, and confidence-building responses. The activity ends with a short debrief on which words or behaviours increased trust and which ones may have increased anxiety.
Section 2- Teaching Core Digital Security Skills	
2.1 Recognising Phishing, Scams and Online Manipulation Patterns	Theoretical part The trainer explains that phishing and scams often follow recurring patterns: urgency, emotional pressure, unexpected requests, suspicious links, fake senders, and demands for passwords, or bank details. Seniors do not need advanced technical knowledge to stay safer; they need to recognise warning signals and learn a few reliable response routines. Practical part Participants analyse simulated emails, scam SMS messages, and fake website prompts, classifying them as safe, suspicious, or not sure. The trainer guides the discussion around visible warning signs and reinforces the idea that “not sure” is already a safe and intelligent response. Participants then practise explaining one suspicious example in senior-friendly language.



Project Partners

2.2 Password Management and Account Protection	Theoretical part The trainer introduces basic password safety principles, including avoiding weak or repeated passwords, protecting key accounts, and understanding why email accounts are especially sensitive. Two-factor authentication is presented as an added layer of protection, but in a practical and non-technical way. The focus remains on routines that are realistic for older adults. Practical part Participants compare weak and stronger password examples and discuss what makes a password safer without making it impossible to remember. They then prepare a short teaching explanation for seniors on password shaping and safer login habits. If appropriate, the trainer may also demonstrate how to introduce two-factor authentication step by step.
2.3 Privacy Settings and Personal Data Protection	Theoretical part The trainer explains what personal data is, why it matters, and how oversharing can happen in social media, messaging apps, online forms, and everyday digital services. The difference between harmless and sensitive information is clarified through concrete examples. Privacy settings are framed as practical tools for safer participation, not as a complex technical burden. Practical part Using screenshots etc, participants review simple



Project Partners

	privacy-setting situations and identify what should be shared, restricted, or kept private. They also discuss how to explain data protection in plain language, especially to learners who feel confused by terms such as permissions, visibility, or access settings.
2.4 Safe Browsing and Secure Use of Everyday Online Services	Theoretical part The trainer presents safe browsing as a set of habits: checking website addresses, recognising suspicious pages, avoiding unsafe downloads, and pausing before proceeding when something feels unclear. Special attention is given to online shopping, banking, healthcare portals, and public services, since these are high-relevance and high-sensitivity areas for older adults. Practical part Participants compare ideas of suspicious websites and discuss which visible clues support safer choices. The trainer then leads a short browsing walkthrough, modelling how to pause, check, and verify before clicking or submitting information. In pairs, participants justify whether they would continue, stop, or seek help in each scenario.
Section 3- Response, Confidence and Evaluation	
3.1 Responding Safely to Suspicious Situations and Mistakes	Theoretical part The trainer explains that a major goal of digital security education is not perfection, but safer responses. Seniors need to know what to do when something feels wrong, when they click by mistake, or when they are unsure



Project Partners

	whether a message is legitimate. Calm response routines are therefore more useful than abstract warnings alone. Practical part Participants work through short “what happened next?” scenarios, such as clicking a suspicious link or receiving a message asking for bank details. For each case, they identify the safest next step and discuss how to teach this without blame or panic. The trainer reinforces calm response habits such as stop, verify, ask for help, and avoid acting under pressure.
3.2 Building Digital Confidence and Safer Habits	Theoretical part The trainer explains that confidence develops through repetition, small successes, and supportive learning experiences. Many seniors avoid digital tools not because they are unable to learn, but because they fear mistakes, fraud, or embarrassment. Digital security teaching should therefore build resilience and reduce dependence, not increase anxiety. Practical part Participants identify simple confidence-building routines they can integrate into their sessions, such as repeating safe-response patterns, celebrating correct decisions, and ending activities with a short reflection on what was learned. They then exchange ideas on how to turn caution into confidence instead of fear into avoidance.
3.3 Evaluating Learning	Theoretical part



Project Partners

Outcomes in Digital Security Training	The trainer presents evaluation as a practical and supportive process. What matters most is whether the learner can recognise common risks, explain a safer choice, and respond more calmly and appropriately in everyday digital situations. Evaluation should therefore remain light, realistic, and closely linked to actual tasks and behaviours. Practical part Participants review simple evaluation tools such as an observation checklist, a short practical task, and a self-reflection sheet. They then select one practical and one reflective method for a digital security activity and briefly justify why these tools are suitable for senior learners.
3.4 Trainer Reflection and Continuous Improvement	Theoretical part The trainer explains that reflection after each session helps improve examples, pacing, language, and materials. Recurrent learner difficulties can reveal where instructions are unclear, where more reassurance is needed, or where activities should be simplified. Reflection is therefore part of quality assurance, not an extra burden. Practical part Participants complete a short reflection prompt on what worked well, what was difficult, and what they would improve in a future digital security session. The activity concludes with a brief sharing of one concrete improvement each participant would carry forward in



Project Partners



	their own practice.
--	---------------------



Project Partners

