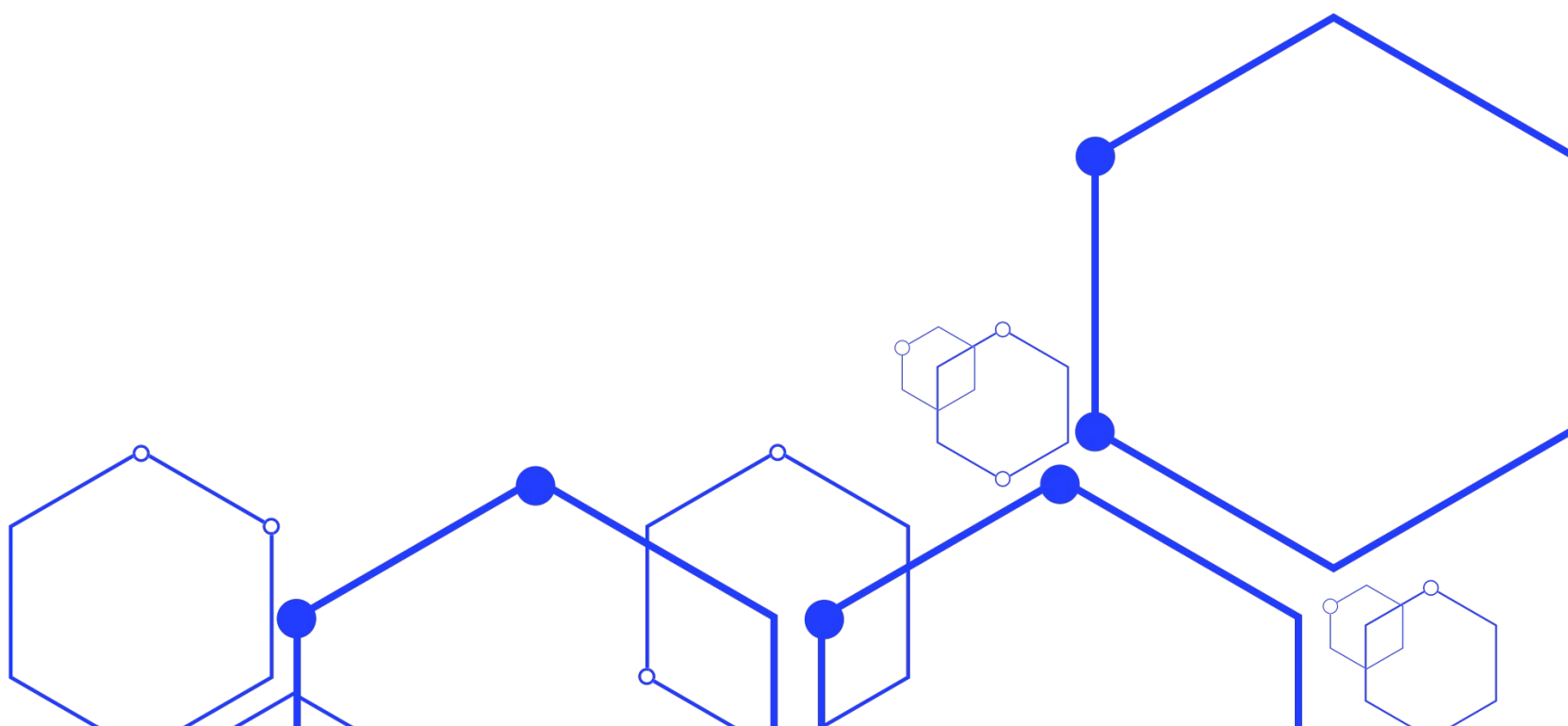




GenerationInfinity

Enhancing digital skills,
competencies & safety in
European older adults & seniors!



**Co-funded by
the European Union**

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 EACEA can be held responsible for them.



GenerationInfinity

Enhancing digital skills,
competencies & safety in
European older adults & seniors!

Project Partners



Municipality of Gotse
Delchev (Bulgaria)



Fundacja "Fundusz
Inicjatyw" (Poland)



Fondazione Università
Adulti Anziani (Italy)



Social Nebula
(Greece)



LJUDSKA UNIVERZA CELJE
Ekipa dobrih ljudi

Ljudska Univerza Celje
(Slovenia)



Co-funded by
the European Union



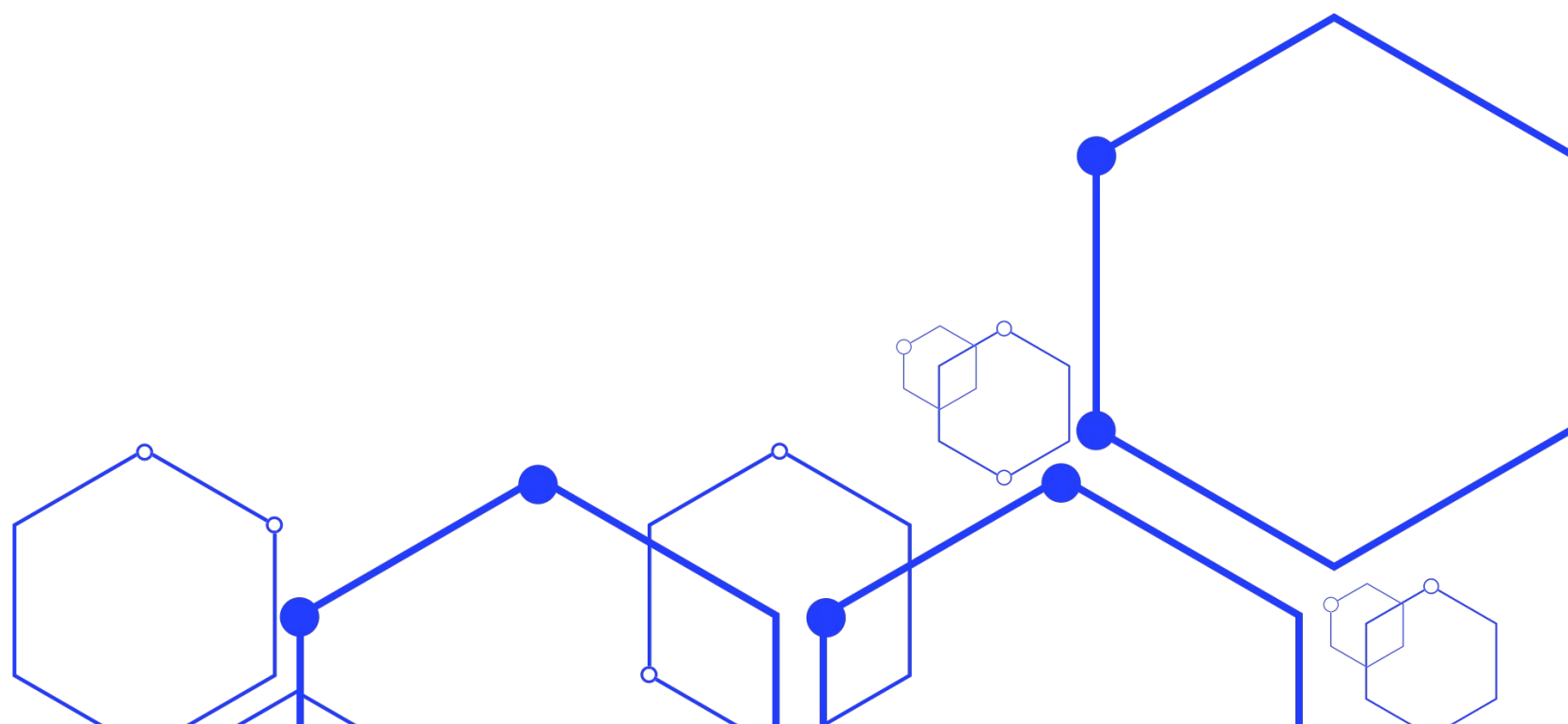
GenerationInfinity

**Enhancing digital skills,
competencies & safety in
European older adults & seniors!**

**WP2 - Train the Trainers Framework
TRAINING MODULE FOR TRAINERS:
Module 6- Digital Security in the Digital Age**

Duration: 2- 3 hours

Partner: Bluechain Research Cooperative



**Co-funded by
the European Union**



GenerationInfinity

What this module helps trainers do!

This module prepares trainers to teach digital security to older adults in a clear, practical, and reassuring way.

- Explain **basic topics** such as phishing, scams, passwords, privacy, and safe browsing
- Design **short activities** based on real online situations
- Teach in ways that reduce **fear** and **build** confidence
- Help learners **respond calmly** when something feels suspicious
- Use simple tools to check learning progress





Module structure

The module is organised into three parts.

1. Section 1- Foundations of Digital Security Learning for Older Adults

Why this topic matters, what seniors struggle with, and how trainers should approach it!

2. Section 2- Teaching Core Digital Security Skills

Phishing, passwords, privacy, and safe browsing!

3. Section 3- Response, Confidence and Evaluation

Safe reactions, confidence-building, assessment, and trainer reflection!



Why digital security matters in everyday life

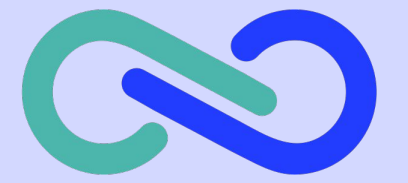
Digital security is not just a technical issue.
For older adults, it is part of everyday digital participation!

Think of the situations they already face:

- ✓ **email and messaging apps**
- ✓ **online banking and shopping**
- ✓ **healthcare portals and e-government services**
- ✓ **social media and everyday browsing**

Our role is to help them see the difference between normal online activity and risky situations, and to build safer habits with confidence.

Understanding older adults' digital safety needs



GenerationInfinity

Digital safety is not only about avoiding danger...
Digital security is part of everyday life...

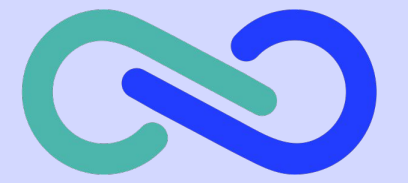


For older adults, it appears in many everyday moments: :

- ☹️ **uncertainty** around **suspicious messages** and links
- ☹️ **confusion** with pop-ups or fake pages
- ☹️ **low confidence and anxiety** when something unexpected appears



What this means for digital security teaching



GenerationInfinity

Main principles:

1. Pacing

Give learners time to notice, think, and respond

2. Repetition

Repeat key safety steps until they feel familiar

3. Visual support

Use visual elements learners can recognise

4. Practical relevance

Connect security to real online situations they face everyday



Remember: Digital security feels easier when it is taught **slowly, clearly & practically!**



The trainer's role in digital security education

In this module, the trainer IS NOT JUST AN INFORMATION PROVIDER!

The trainer is:

- ★ **a facilitator**
- ★ **a safety guide**
- ★ **a confidence-builder**

⇒who supports learning, safety, and confidence!

The trainer's role in digital security education

Therefore the Trainer should:

- ➡ Use **relevant, realistic examples** and **protect privacy** when using screenshots or demo materials.
- ➡ **Slow the process down** when needed and explain the “why” behind safer choices.
- ➡ **Reinforce safe responses** without shame, so learners feel supported when practising digital safety.

 *Try to use simulated materials and try to avoid real passwords, bank details, or personal information!*

Communication, Reassurance and Trust-Building

The way digital security is explained can either:

Support learning

Quietly block learning

Older adults engage more easily when the trainer uses:

- ♥ **calm language**
- ♥ **plain explanations**
- ♥ **a learning atmosphere** where uncertainty feels normal and for sure, NOT EMBARASSING!

Communication, Reassurance and Trust-Building

Trainers should avoid:

- ➡ Jargon
- ➡ Fear-based training
- ➡ Rushed explanations

What supports learning more effectively:

- ➡ Visible patience
- ➡ Repetition
- ➡ Simple language

Communication, Reassurance and Trust-Building

A particularly important message to reinforce is that **“not sure”**
is a **valid, acceptable and safe** response!

It gives learners permission to *pause, think*, and *ask* for help instead of reacting under pressure!



Recognising Phishing, Scams and Online Manipulation Patterns

The goal is **NOT** to turn older adults into **technical experts**!

The real aim is to help them recognise recurring warning patterns.

Suspicious messages may look **different**, but they often use the **same tactics**!



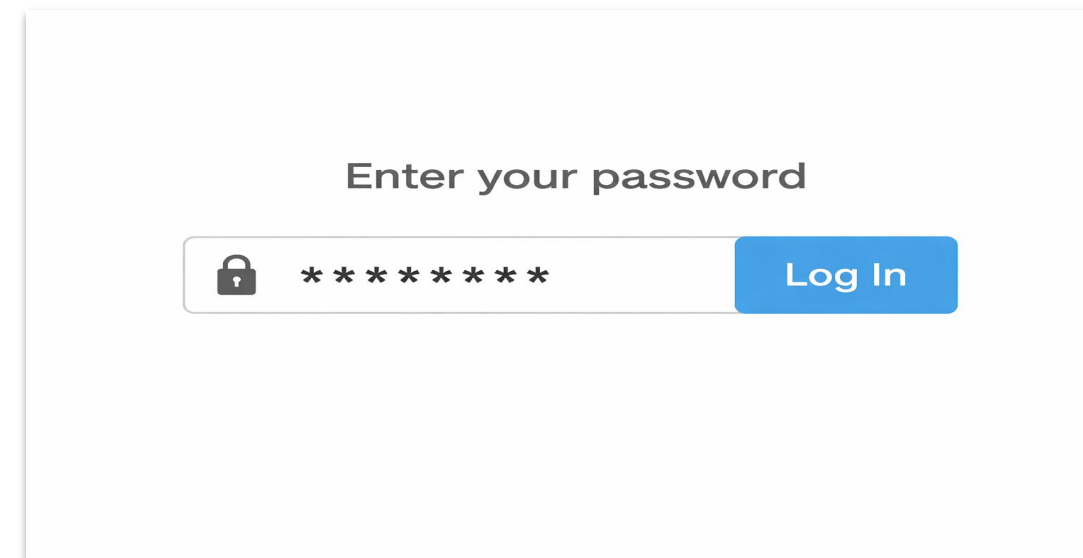


Common warning patterns ...

Suspicious messages often rely on:

-  **urgency** and **secrecy**
-  requests for **passwords**, **codes**, **banking details**, or **personal information**
-  emotional **pressure**
-  **fake senders** and **suspicious links**

Learners do not need to know everything!
They need to be able to notice warning signs,
then **slow down**,
and then follow reliable response habits.



Password Management and Account Protection

Trainers should move beyond general advice and **focus on routines** that older adults can actually use in their daily lives...in practical and realistic ways!

- *why weak or repeated passwords create risk?*
- *why some accounts are especially sensitive?*
- *how stronger password habits improve protection?*

The aim here is **NOT to overwhelm** learners with rules!



GenerationInfinity

Stronger habits, step by step !

Give particular attention to:

- 📱 **email accounts**
- 📱 **banking access**
- 📱 **public service accounts**



These accounts often serve as gateways to other personal information and services.



Stronger habits, step by step !

Example 👉 Two-Factor Authentication (2FA)

Two-factor authentication **is not another complicated rule**, it's a main **safety step** to important accounts.

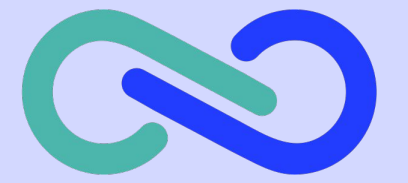
It helps protect learners even if a password is:

- ***weak***
- ***repeated***
- ***exposed***

Small tip:

Use 2FA especially for **email accounts, banking access, public service accounts**.

Privacy Settings and Personal Data Protection



GenerationInfinity

Privacy is often misunderstood as a technical or legal issue, when in reality it is a very practical part of everyday digital safety!

Help them understand:

What personal data is

Why it matters

How oversharing can happen in digital environments (e.g. social media)



Privacy Settings and Personal Data Protection

Privacy Settings & Personal Data Protection



Understanding what to share and what not to share by explaining the difference between: :

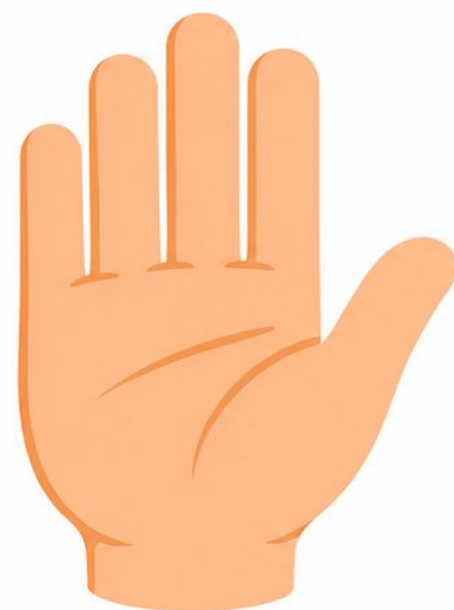
- information that is harmless
- information that is sensitive
- information that should not be shared casually online.

Privacy settings should therefore be presented **not as complicated topics** to fear, but as **tools** that help people participate more safely and with more confidence!

Safe Browsing and Secure Use of Everyday Online Services

Adopt a set of habits rather than a single skill!

Older adults need support in learning how to:



1. Pause



2. Observe



3. Make safer choices

Slow down and verify before proceeding

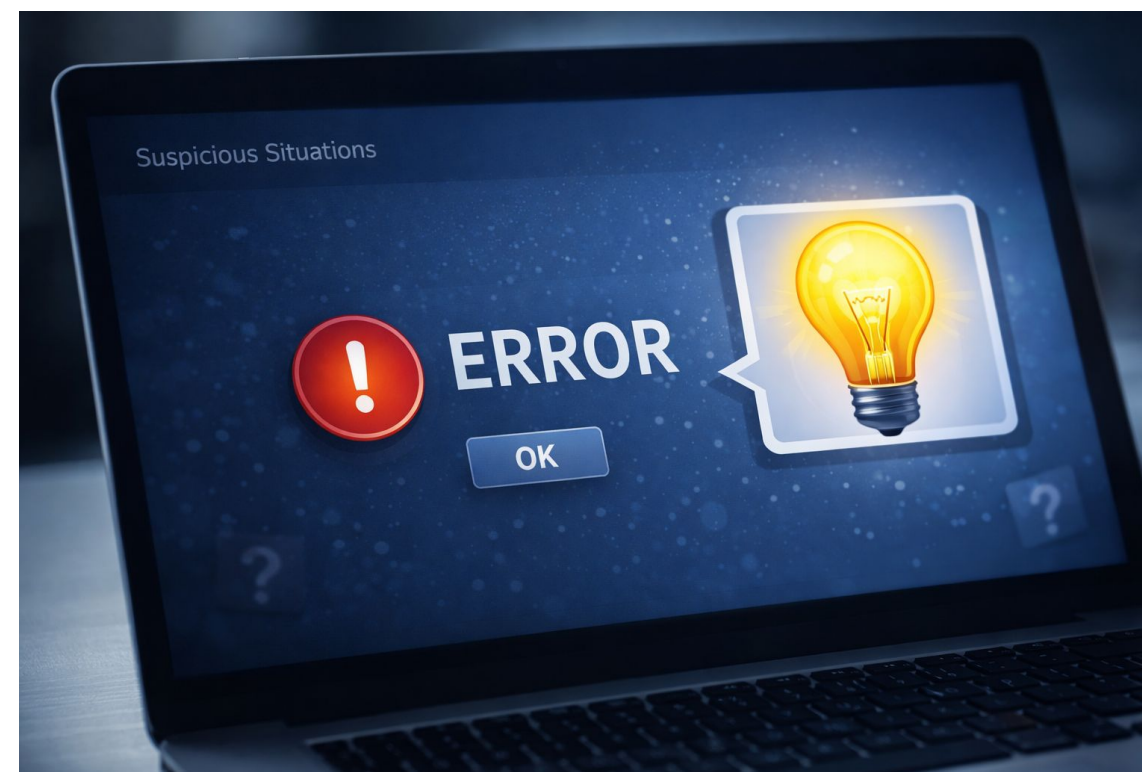


Trainers should model a careful way of moving through online environments.

Learners should look more carefully at:

- website addresses
- login pages
- pop-ups
- redirections

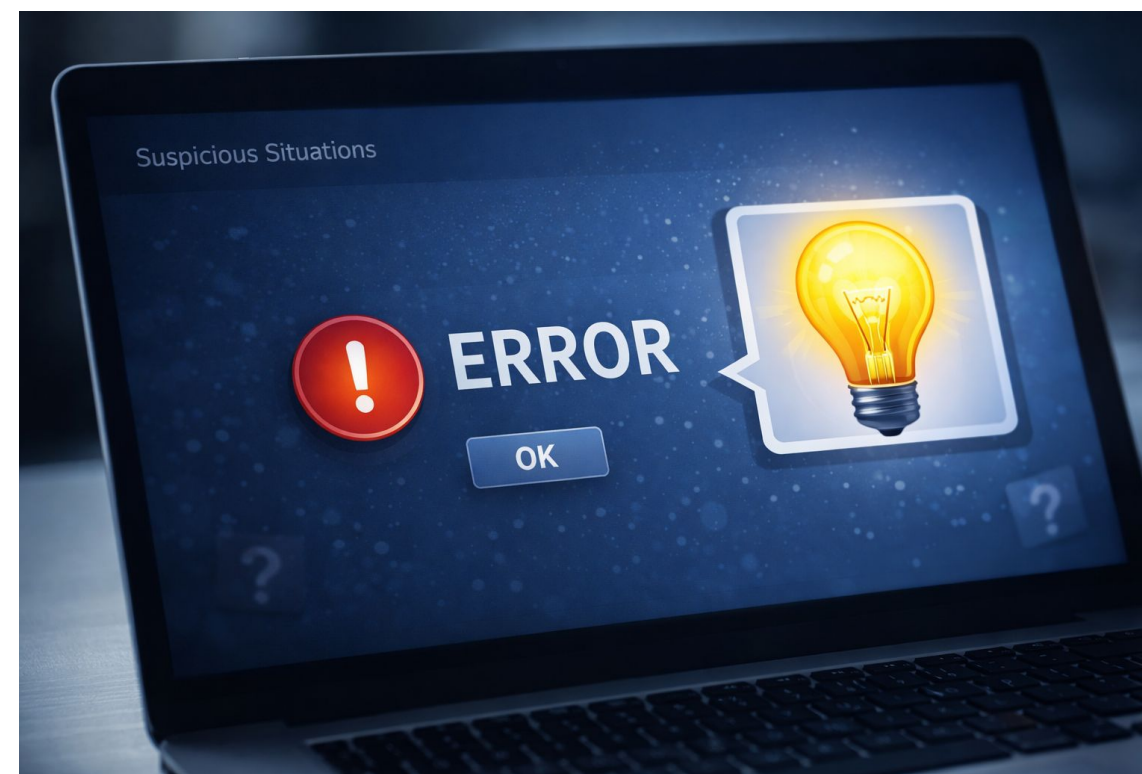
Remember: Digital security is not about speed!



Responding Safely to Suspicious Situations and Mistakes!

A key message in digital security education **is that safe participation does not depend on never making mistakes!!!**

Older adults need practical guidance not only for **prevention**, but also for those moments of uncertainty that create panic: a suspicious link has been opened, a strange message has appeared, or information may have been shared by mistake!

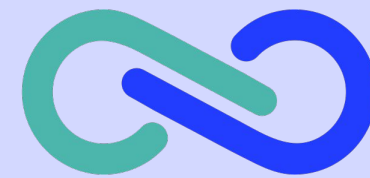


Simple response routines

The emphasis should remain on:

- Pausing & verifying the situation
- Avoiding impulsive action
- Seeking help when needed

This moves learners away from fear-based reactions and towards calmer, safer decision-making.



GenerationInfinity

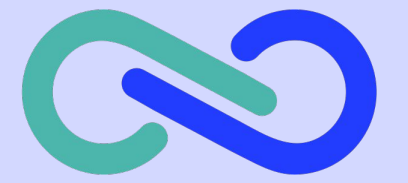
Building Digital Confidence and Safer Habits

Confidence in digital security does not appear all at once!

It develops:

- **gradually**
- **through repetition and visible progress**
- **through the experience of handling small risks more successfully over time**





GenerationInfinity

Why safer habits matter?

Do older adults withdraw from digital tools because they are unable to learn? No!

They often withdraw because they associate digital environments with:



fraud



mistakes



embarrassment





Evaluating Learning Outcomes in Digital Security Training

Evaluation in digital security training should remain:

1. **Supportive**
2. **Realistic**
3. **Closely connected to what learners can actually do.**



Keep it light: observation, short practical task, brief quiz, or simple self-reflection prompt



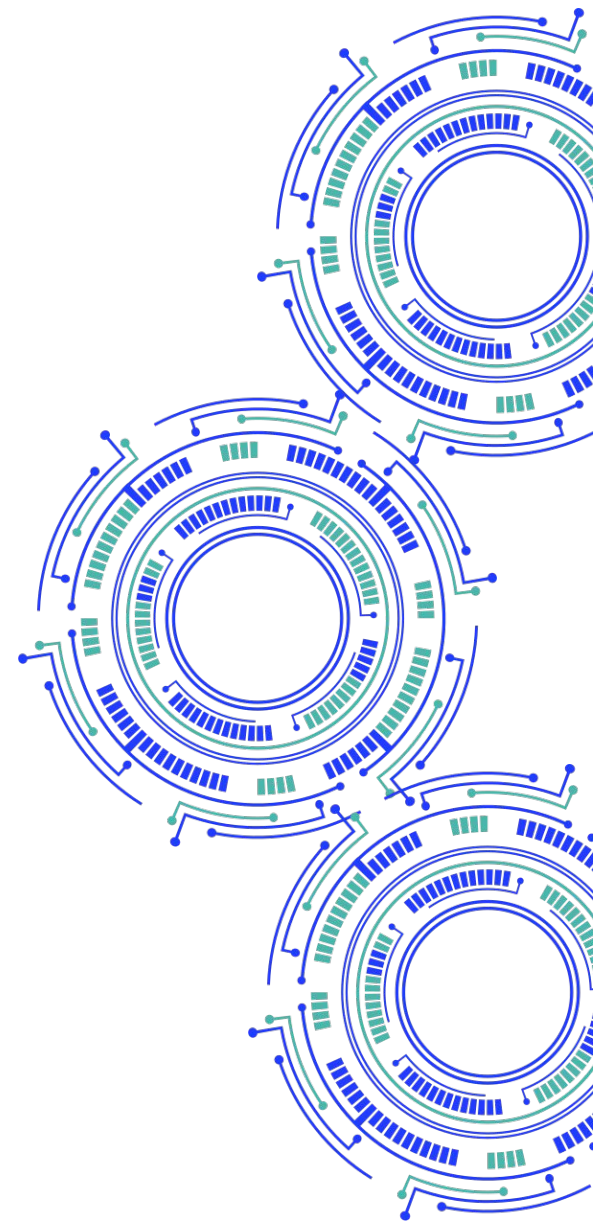
GenerationInfinity

Trainer Reflection and Continuous Improvement

Reflection after each session helps trainers look beyond whether an activity was completed.

It helps them consider:

- which examples worked well
- where confusion appeared
- which moments created anxiety





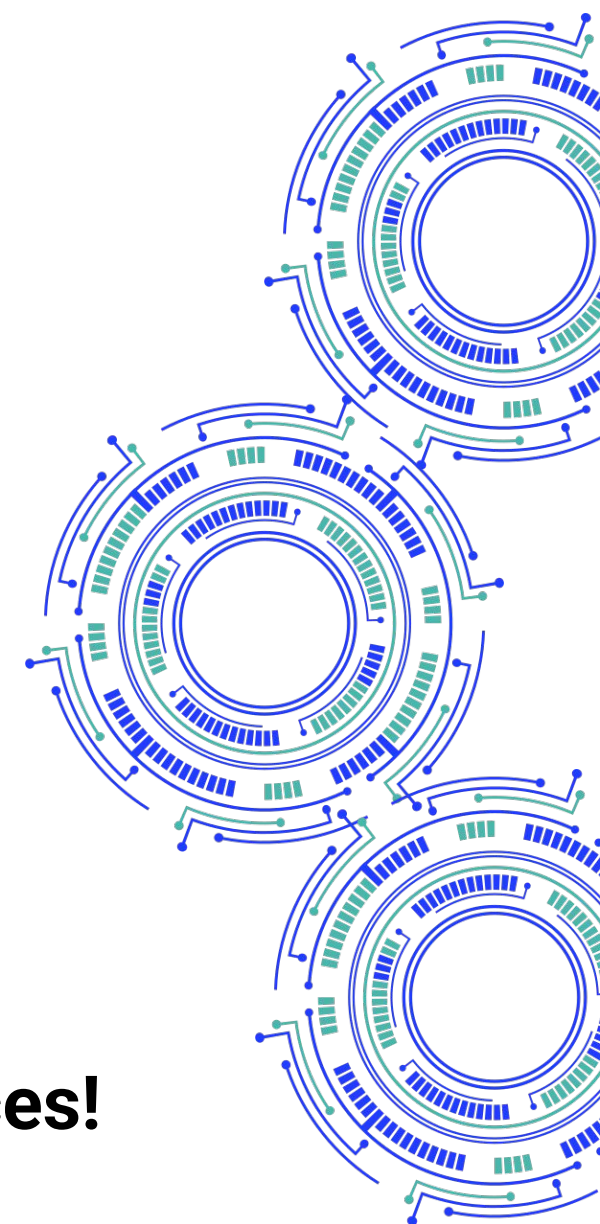
GenerationInfinity

Improving the next session !

Trainer reflection helps refine:

- pacing
- language
- materials
- choice of examples

Each session can contribute to stronger and more reusable teaching resources!



Concluding Perspective

Teaching digital security to older adults is not simply about transferring information.

It helps learners participate in digital life with:

- greater safety
- more confidence

Effective training combines **practical knowledge with reassurance, structure, and respect for learners' emotional realities.**



A glance at the wider purpose of this module

The trainer's role is both educational and enabling!

When risks are explained clearly and calm responses are practised, digital security stops feeling like a threat!

It becomes a tool for:

- safer choices!
- more confidence!
- greater independence online!



GenerationInfinity



Thank you!





GenerationInfinity

Find us



generationinfinity.eu



Generation Infinity

The Generation Infinity Project 2024-1-BG01-KA220-ADU-000248972



Co-funded by
the European Union