Co-funded by the European Union

DIGITAL ERA

TRAINING PROGRAM
developed by Centro Consorzi /Partner Organisation/

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

"Cybersecurity in Everyday Life: How to Recognise Threats and Protect Our Personal Data"

TARGET GROUP

Adults 30+
Active online users
Employees in the public and private sector
Parents
Self-employed individuals and small entrepreneurs

GENERAL OBJECTIVE

Development of critical digital thinking that enables:

- recognition of online threats in real time
- conscious management of personal and sensitive data
- making informed decisions, rather than acting out of fear or complete distrust of technology

PEDAGOGICAL AND SCIENTIFIC FRAMEWORK

The training is based on:

- behavioural cybersecurity (human-centred cybersecurity)
- cognitive psychology (how people make decisions under risk)
- information asymmetry and social engineering
- risk management principles (probability × impact)

Key thesis:

Most security breaches are not technological, but human.

TRAINING STRUCTURE

MODULE 1

How Digital Risk Works: Why "Reasonable People" Become Victims

1.1. What an Online Threat Really Is

– not a "virus", but a scenario
– threat ≠ technology
– threat = person + motivation + access + trigger

Example: An email itself is not dangerous. The reaction it provokes is.

1.2. Why Adults Are Vulnerable (Scientific Explanation)
– trust built offline and transferred online
– multitasking and cognitive fatigue
– authority signals ("bank", "public institution", "boss")

1.3. Attack Model (Attack Chain)
– information gathering
– manipulation
– pressure for rapid action
– exploitation of the mistake

MODULE 2
Social Engineering: The Psychology Behind Fraud

2.1. How Fraudsters "Read" People
Main psychological levers: fear; guilt; urgency; authority; reward

Important: No one is "stupid" when professionally manipulated.

2.2. Phishing – Not as Technology, but as Communication
– linguistic markers
– logical inconsistencies
– emotionally charged formulations

2.3. Why It "Looks Real"
– cloned websites
– compromised real accounts
– use of real data (data leaks)

MODULE 3
Personal Data: What Really Has Value

3.1. What Personal Data Are in 2026
Not only: personal ID number, address, but also: habits; location; social connections; behaviour patterns

3.2. Data as a "Puzzle"
One fragment ≠ problem

Combination of fragments = profile

3.3. Why "I Have Nothing to Hide" Is a Dangerous Argument
– automated decision-making
– profiling
– denial of services

MODULE 4
Passwords, Devices and Clouds – The Real Minimum That Makes Sense

4.1. The Password as a Key, Not a Secret
– length > complexity
– reuse = systemic risk

4.2. Two-Factor Authentication – When It Helps and When It Does Not
– SIM swap attacks
– push fatigue

4.3. The Smartphone – The Most Vulnerable Device
– applications with excessive permissions
– public Wi-Fi networks
– automatic backups

MODULE 5
Social Networks and Communication Platforms

5.1. How Social Networks Collect More Than We Publish
– metadata
– interactions
– "likes"

5.2. Fake Profiles and Deepfakes
– what can no longer be visually proven
– why voice is also no longer evidence

5.3. Family and Parental Cybersecurity
– children as an entry point
– shared devices

MODULE 6

How to Think When We Are Not Sure (Practical Framework)

6.1. Rule "Pause – Check – Decide"
– delay as protection
– verification through an independent channel

6.2. Minimal Personal Security Strategy
– what I protect most
– where I am most vulnerable
– what I accept as an acceptable risk

TRAINING FORMAT

Real-life case studies
Analysis of real scenarios
Group discussions
Exercises for "pattern recognition", not checklists