

DIGITAL ERA

Digital Skills and Cybersecurity Training Course for Adults and Elderly People

CO-FUNDED BY THE EUROPEAN UNION

Co-funded by the European Union

BASIC DIGITAL SKILLS AND INDEPENDENT USE OF TECHNOLOGY MODULE 2

COMPLEMENTARY EDUCATIONAL MATERIAL

PRACTICAL DIGITAL SKILLS, ARTIFICIAL INTELLIGENCE AND E-SERVICES FOR ADULT LEARNERS

DEVELOPED BY: ASSOCIATION FOR SUPPORT OF ELDERLY PEOPLE OF RETIREMENT AGE "POWER"

DIGITAL ERA: DIGITAL SKILLS AND CYBERSECURITY TRAINING COURSE FOR ADULTS AND ELDERLY PEOPLE

PROJECT NO.: 2025-1-BG01-KA210-ADU-000352026

PROGRAMME: ERASMUS+

ACTION: KA210-ADU – SMALL-SCALE PARTNERSHIPS IN ADULT EDUCATION

Educational resource for adult learners, including older adults and people with limited digital experience.

2026

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.

Co-funded by the European Union

Contents

Overall Learning Objective 6

Expected Learning Outcomes 6

2.1. What Is Artificial Intelligence? 7

2.1.1. Introduction to Artificial Intelligence 7

2.1.2. Artificial Intelligence in Everyday Technologies 8

2.1.3. Traditional Software and Artificial Intelligence 9

2.1.4. Understanding Generative Artificial Intelligence 10

2.1.5. How AI Systems Learn from Data 10

2.1.6. What Artificial Intelligence Can Do 11

2.1.7. What Artificial Intelligence Cannot Reliably Do 11

2.1.8. Artificial Intelligence and Human Decision-Making 12

2.1.9. Opportunities for Older Adults 12

2.1.10. Common Misconceptions About Artificial Intelligence 13

2.1.11. Practical Learning Activity: Recognising AI in Everyday Life 14

2.1.12. Learning Unit Summary 14

2.2. Practical AI Applications in Everyday Life 15

2.2.1. Introduction to Practical AI Use 15

2.2.2. AI for Writing Everyday Messages 15

2.2.3. AI for Simplifying Complex Information 16

2.2.4. AI for Summarising Information 17

2.2.5. AI for Translation and Language Assistance 17

2.2.6. AI for Personal Organisation 18

2.2.7. AI for Travel and Everyday Planning 19

2.2.8. AI for Lifelong Learning 19

2.2.9. AI for Generating Ideas 20

2.2.10. AI and Accessibility Support 21

2.2.11. Choosing Appropriate AI Tools 21

2.2.12. Reviewing AI-Generated Results 22

2.2.13. Practical Exercise: Preparing a Simple Email with AI 22

2.2.14. Practical Exercise: Simplifying Digital Terminology 23

2.2.15. Practical Exercise: Creating a Personal Activity Plan 23

2.2.16. Practical Exercise: Comparing AI Responses 24

2.2.17. Practical Exercise: Identifying Information 24

Co-funded by the European Union

2.2.18. Learning Unit Summary 25
2.3. Effective Interaction with AI Tools 25
2.3.1. Introduction to Effective AI Communication 25
2.3.2. Understanding the Concept of a Prompt 25
2.3.3. The Four Elements of a Useful Prompt 26
2.3.4. Comparing Unclear and Clear Instructions 27
2.3.5. Asking AI to Use Simple Language 28
2.3.6. Requesting Step-by-Step Instructions 28
2.3.7. Providing Appropriate Context 29
2.3.8. Improving an AI Response Through Follow-Up Questions 29
2.3.9. Asking AI to Compare Alternatives 30
2.3.10. Requesting Examples and Practice Questions 30
2.3.11. Recognising When a Prompt Is Too Broad 31
2.3.12. Avoiding Unnecessary Personal Information 31
2.3.13. Evaluating the Quality of an AI Response 31
2.3.14. Practical Exercise: Improving a Prompt 32
2.3.15. Practical Exercise: Learning Through Follow-Up Questions 32
2.3.16. Practical Exercise: Preparing a Structured Request 32
2.3.17. Learning Unit Summary 33
2.4. AI Limitations, Privacy and Responsible Use 33
2.4.1. Introduction to Responsible AI Use 33
2.4.2. Understanding AI-Generated Errors 33
2.4.3. What Are AI Hallucinations? 34
2.4.4. Why AI Responses Require Verification 34
2.4.5. Distinguishing Between Low-Risk and High-Risk AI Tasks 35
2.4.6. Personal Data and Artificial Intelligence 36
2.4.7. Sensitive Information That Should Not Be Entered into AI Exercises 36
2.4.8. Using Fictional Data and Placeholders 37
2.4.9. Understanding AI Bias 38
2.4.10. AI and Stereotypes About Older Adults 38
2.4.11. Understanding the Limits of AI Personalisation 38
2.4.12. AI and Professional Advice 39
2.4.13. Transparency and Awareness of AI-Generated Content 39
2.4.14. Responsible Use of AI-Generated Images and Media 40
2.4.15. Recognising Manipulative AI-Based Services 40
2.4.16. Responsible Decision-Making Framework 41

Co-funded by
the European Union

2.4.17. Practical Exercise: Identifying AI Hallucinations 41
2.4.18. Practical Exercise: Protecting Personal Information 42
2.4.19. Practical Exercise: Evaluating AI Advice 42
2.4.20. Practical Exercise: Responsible AI Decision-Making 43
2.4.21. Learning Unit Summary 43
2.5. Artificial Intelligence, Disinformation and Online Fraud 44
2.5.1. Introduction to AI-Related Information Risks 44
2.5.2. Understanding Misinformation and Disinformation 44
2.5.3. How Artificial Intelligence Can Be Used to Create Misleading Content 45
2.5.4. Understanding Deepfakes 45
2.5.5. Why Deepfakes Can Be Difficult to Recognise 46
2.5.6. AI-Generated Images and False Visual Evidence 47
2.5.7. AI Voice Cloning and Impersonation Fraud 47
2.5.8. AI-Enhanced Phishing Messages 48
2.5.9. Fraudulent Investment and Financial Offers 48
2.5.10. Fraudulent Online Shopping Content 49
2.5.11. Manipulative Messages and Emotional Pressure 49
2.5.12. A Practical Verification Method 50
2.5.13. Using Search Engines for Verification 51
2.5.14. Understanding Reverse Image Search 51
2.5.15. Limitations of Automated AI-Detection Tools 51
2.5.16. Responsible Sharing of Digital Content 52
2.5.17. Responding to Suspected AI-Related Fraud 52
2.5.18. Practical Exercise: Recognising a Deepfake Scenario 53
2.5.19. Practical Exercise: Voice Impersonation Fraud 54
2.5.20. Practical Exercise: Evaluating an Online News Claim 54
2.5.21. Practical Exercise: Identifying Manipulative Messages 54
2.5.22. Learning Unit Summary 55
2.6. Practical AI Exercises and Skills Assessment 55
2.6.1. Purpose of Practical Assessment 55
2.6.2. Assessment Objectives 55
2.6.3. Initial AI Knowledge Assessment 56
2.6.4. Practical Task 1: Recognising AI Applications 56
2.6.5. Practical Task 2: Creating a Clear Prompt 56
2.6.6. Practical Task 3: Improving an AI Response 57
2.6.7. Practical Task 4: Using AI for Everyday Communication 57

Co-funded by
the European Union

2.6.8. Practical Task 5: Identifying AI Hallucinations 58
2.6.9. Practical Task 6: Protecting Personal Information 58
2.6.10. Practical Task 7: Recognising AI-Related Fraud 58
2.6.11. Integrated Practical Scenario: Using AI Responsibly 59
2.6.12. Practical Assessment Criteria 59
2.6.13. Levels of Achievement 60
2.6.14. Trainer Assessment Checklist 60
2.6.15. Learner Self-Assessment 61
2.6.16. Reflection and Discussion 61
2.6.17. Trainer Feedback and Individual Recommendations 62
2.6.18. Continued Independent Learning 62
2.6.19. Completion of Module 2 63
2.6.20. Overall Module Conclusion 63
Module Overview 63
Overall Learning Objective 64
Expected Learning Outcomes 64

Co-funded by
the European Union

Module Overview

Artificial intelligence is increasingly integrated into digital technologies used for communication, information searches, education, personal organisation, and access to services.

Many adults already encounter AI-supported functions without necessarily recognising them as applications of artificial intelligence.

Examples include automatic translation, voice assistants, personalised recommendations, navigation systems, and tools that generate written content.

At the same time, the rapid development of artificial intelligence creates new challenges related to information reliability, privacy, cybersecurity, and digital manipulation.

For adults with limited digital experience, these developments may create uncertainty or additional barriers to digital participation.

Module 2 provides an accessible and practically oriented introduction to artificial intelligence.

It is designed to help adult learners understand basic AI concepts, recognise common applications, use selected AI tools responsibly, and evaluate AI-generated information critically.

The module does not require programming knowledge or advanced technical competencies.

Instead, it focuses on everyday situations in which artificial intelligence may provide useful assistance.

The module is organised into six learning units:

2.1. What Is Artificial Intelligence?
2.2. Practical AI Applications in Everyday Life
2.3. Effective Interaction with AI Tools
2.4. AI Limitations, Privacy and Responsible Use
2.5. Artificial Intelligence, Disinformation and Online Fraud
2.6. Practical AI Exercises and Skills Assessment

Overall Learning Objective

To develop adult learners' basic understanding of artificial intelligence and strengthen their ability to use AI-supported digital tools practically, critically, responsibly, and safely in everyday situations.

Expected Learning Outcomes

By the end of the module, learners should be able to:

- Explain the basic concept of artificial intelligence in understandable terms.

Co-funded by the European Union

- Recognise common examples of AI in everyday digital technologies.
- Identify situations in which AI tools may provide practical assistance.
- Use an appropriate AI tool to complete a simple task.
- Formulate clear questions and instructions.
- Review and improve AI-generated responses.
- Recognise that AI systems may produce inaccurate or misleading information.
- Protect personal and sensitive information when using AI applications.
- Identify potential risks associated with AI-generated content.
- Apply critical thinking and independent verification when using artificial intelligence.

2.1. What Is Artificial Intelligence?

2.1.1. Introduction to Artificial Intelligence

Artificial intelligence, commonly abbreviated as AI, refers to computer systems designed to perform tasks that involve capabilities such as recognising patterns, processing language, generating content, making predictions, or supporting decisions.

These systems use computational methods and data to produce results that may resemble certain aspects of human reasoning or communication.

Artificial intelligence does not necessarily mean that a computer thinks or understands the world in the same way as a human being.

Instead, AI systems process information using mathematical models and computational techniques.

For adult learners, the most useful starting point is to understand artificial intelligence through familiar examples rather than complex technical explanations.

AI can be described as technology that allows computers and digital applications to perform certain tasks that would otherwise require substantial human effort.

Examples include:

- Translating a sentence into another language.
- Recognising spoken words.
- Suggesting a route to a destination.
- Identifying objects in photographs.
- Summarising a written document.
- Generating a draft message.
- Answering questions in conversational language.

These functions illustrate how artificial intelligence can support everyday digital activities.

Co-funded by
the European Union



What Is Artificial Intelligence?

2.1.2. Artificial Intelligence in Everyday Technologies

Artificial intelligence is not limited to specialised scientific laboratories or advanced computer systems.

It is increasingly incorporated into applications used by ordinary consumers.

Smartphone functions

Some smartphones use AI-supported features for photography, speech recognition, text prediction, and image organisation.

Navigation applications

Navigation services may use predictive algorithms and other computational methods to estimate travel conditions and suggest routes.

Translation tools

AI-supported translation applications can assist users in understanding text written in unfamiliar languages.

Voice assistants

Voice assistants can interpret spoken requests and perform selected tasks, such as setting reminders or providing information.

Online recommendations

Some digital platforms use algorithms to recommend products, videos, music, or other content based on available information about user activity.

Digital accessibility

AI-supported functions may assist with speech-to-text conversion, text recognition, and other accessibility-related tasks.

Co-funded by
the European Union

These examples demonstrate that artificial intelligence can be integrated into familiar digital activities without requiring users to understand the underlying technical processes.



Voice Assistant

2.1.3. Traditional Software and Artificial Intelligence

Traditional software and AI-supported applications may perform similar tasks, but their methods can differ.

Traditional software commonly follows predefined instructions established by its developers.

For example, a basic calculator performs mathematical operations according to established rules.

An AI-supported system may identify patterns in data, interpret less structured requests, or generate new content based on information learned during development.

A simple comparison can help learners understand this distinction.

Traditional calculator

The user enters a mathematical operation, and the calculator produces the corresponding result.

AI conversational assistant

The user may describe a problem in ordinary language and request an explanation, calculation, or suggested approach.

The AI system interprets the request and generates a response.

However, the flexibility of AI systems does not guarantee that every response will be correct.

This distinction is important because users should not assume that an AI-generated answer has been independently verified.

Co-funded by
the European Union

2.1.4. Understanding Generative Artificial Intelligence

Generative artificial intelligence refers to AI systems that can produce new content in response to user instructions.

Depending on the system, this content may include:

- Written text.
- Images.
- Audio.
- Video.
- Computer code.
- Summaries and explanations.
- Suggested plans and structured information.

A generative AI tool may be able to prepare a draft email, explain an unfamiliar concept, or summarise a document.

Some systems can also generate illustrations or other multimedia content.

The trainer should explain that generated content is produced computationally and may contain inaccuracies, omissions, or invented details.

Users remain responsible for reviewing the information before relying on it.



AI Assistant (Chatbot)

2.1.5. How AI Systems Learn from Data

Many artificial intelligence systems are developed through processes that involve analysing large amounts of data.

Co-funded by
the European Union

During training, computational models identify patterns and relationships that can later be used to process new inputs.

For example, a language model may learn statistical relationships between words, phrases, and other elements of language.

When a user enters a question, the system generates a response based on its computational processing of the request.

This does not mean that the system possesses human experiences, personal judgement, or an independent understanding of every subject.

Participants should understand that AI systems can produce convincing responses even when the underlying information is incomplete or incorrect.

The programme therefore emphasises the importance of critical evaluation.

2.1.6. What Artificial Intelligence Can Do

Artificial intelligence can support a wide range of everyday activities.

For example, AI tools may help users:

- Understand unfamiliar terminology.
- Prepare written messages.
- Summarise general information.
- Translate simple texts.
- Organise personal activities.
- Generate ideas for educational or creative tasks.
- Compare general information.
- Practise communication in another language.
- Explore alternative explanations of a subject.

These functions can be particularly useful for adults who wish to develop greater confidence in digital environments.

However, AI should be understood as an assistance tool rather than a guaranteed source of accurate information.

2.1.7. What Artificial Intelligence Cannot Reliably Do

Understanding AI limitations is an essential component of digital literacy.

AI systems may produce incorrect statements, misunderstand questions, or generate information that appears plausible but is not supported by reliable evidence.

They may also lack access to current information or the specific context required for an accurate response.

Participants should understand that AI cannot automatically guarantee:

- Factual accuracy.

Co-funded by
the European Union

- Complete or current information.
- Reliable professional advice.
- Correct interpretation of every personal situation.
- Protection of information entered by users.
- Freedom from bias or misleading content.

AI-generated responses should be treated as information requiring appropriate evaluation.

This is particularly important in matters involving health, legal rights, financial decisions, and personal safety.

2.1.8. Artificial Intelligence and Human Decision-Making

Artificial intelligence can support decision-making by organising information, presenting alternatives, and helping users understand unfamiliar subjects.

However, the final responsibility for important decisions remains with the individual or the relevant qualified professional.

For example, an AI tool may explain general financial terminology, but it should not be treated as a substitute for professional financial advice.

Similarly, AI may provide general information about health-related topics, but medical decisions should be based on appropriate professional guidance.

The programme encourages participants to use AI as a supportive resource while maintaining independent judgement.

2.1.9. Opportunities for Older Adults

Artificial intelligence may provide practical benefits for older adults and individuals with limited digital experience.

Potential applications include:

Simplifying information

AI tools may explain unfamiliar digital terms in plain language.

Supporting written communication

Users may request assistance preparing a polite email or formal message.

Language assistance

Translation and language explanation functions may support communication and access to information.

Personal organisation

AI tools may help prepare simple schedules, lists, or reminders, depending on the available application.

Educational support

Co-funded by
the European Union

Learners may request additional explanations or examples when studying unfamiliar topics.

Accessibility support

Selected AI-supported functions may assist with speech recognition, reading, or other accessibility needs.

These opportunities should be presented realistically, with appropriate attention to privacy, accuracy, and the limitations of individual tools.



Learning Digital Skills

2.1.10. Common Misconceptions About Artificial Intelligence

Adult learners may encounter exaggerated or misleading claims about artificial intelligence.

The programme should address several common misconceptions.

Misconception 1: AI always provides correct answers.

AI systems can produce inaccurate or fabricated information.

Misconception 2: AI understands everything like a human being.

AI systems process information computationally and do not necessarily possess human understanding or judgement.

Misconception 3: AI can replace every professional.

AI may support certain professional tasks, but specialised expertise and human responsibility remain important.

Misconception 4: Everything generated by AI is safe to use.

AI-generated content may contain errors, inappropriate suggestions, or privacy-related risks.

Misconception 5: AI is too complicated for older adults.

Co-funded by
the European Union

Many AI applications are designed for interaction through ordinary language and can be introduced through accessible, practical exercises.

The objective is to develop a balanced understanding that recognises both the opportunities and limitations of AI.

2.1.11. Practical Learning Activity: Recognising AI in Everyday Life

Learning objective: To identify familiar examples of artificial intelligence.

Activity description:

The trainer presents several digital activities:

1. Using a calculator.
2. Asking a voice assistant for information.
3. Receiving an automatic translation.
4. Writing a message with a traditional text editor.
5. Using an AI tool to summarise a paragraph.
6. Receiving personalised content recommendations.

Participants discuss which activities may involve artificial intelligence and why.

The trainer explains that some digital services combine traditional software functions with AI-supported components.

Reflection questions:

- Have you used an AI-supported application before?
- Which examples are familiar to you?
- Which AI functions could be useful in your everyday life?
- What concerns do you have about artificial intelligence?
- Why is it important to verify AI-generated information?

Expected learning result: Participants develop a basic understanding of artificial intelligence and recognise examples of its practical use.

2.1.12. Learning Unit Summary

This learning unit introduces artificial intelligence through clear explanations and familiar everyday examples.

Participants learn what AI is, how it differs from traditional software, and how AI-supported functions appear in commonly used digital technologies.

The unit also introduces generative AI, practical opportunities, limitations, and the importance of human judgement.

The expected educational outcome is a balanced understanding of artificial intelligence that supports informed and responsible use.

Co-funded by
the European Union

2.2. Practical AI Applications in Everyday Life

2.2.1. Introduction to Practical AI Use

Artificial intelligence can support many everyday activities that involve information, communication, organisation, and learning.

For adult learners, practical examples are particularly important because they demonstrate how unfamiliar technologies may provide meaningful assistance.

This learning unit introduces accessible applications of AI without requiring advanced technical knowledge.

The focus is on tasks that can be performed through simple instructions using ordinary language.

Participants should understand that AI tools differ in their available functions, access requirements, costs, and privacy arrangements.

The trainer should select appropriate applications and explain relevant limitations before practical use.



Everyday Uses of AI

2.2.2. AI for Writing Everyday Messages

One of the most accessible uses of generative AI is assistance with written communication.

An AI tool may help users prepare drafts of emails, messages, invitations, or requests for information.

Co-funded by the European Union

For example, a participant may wish to contact a community organisation but feel uncertain about how to structure the message.

A possible instruction is:

Write a short and polite email asking a community centre whether it offers computer courses for adults.

The AI tool may generate a draft containing a greeting, explanation of the request, and closing.

The learner should then review the text, correct any inaccuracies, and adapt it to the intended situation.

Important principle: AI-generated messages should not be sent automatically without review.

The user remains responsible for the accuracy, appropriateness, and final content of the communication.



Writing with AI

2.2.3. AI for Simplifying Complex Information

Adults may encounter unfamiliar terminology in digital services, administrative information, or educational materials.

AI tools can sometimes help explain complex concepts in more accessible language.

For example:

Explain what two-factor authentication means using simple language and an everyday example.

The generated response may provide a basic explanation of account protection and describe how an additional verification step can improve security.

Co-funded by
the European Union

Another example is:

Explain the difference between a website and a mobile application for someone who is learning to use a smartphone.

Such exercises can support understanding and reduce uncertainty.

However, simplified explanations may omit important details.

Participants should be encouraged to consult reliable sources when accuracy is essential.

2.2.4. AI for Summarising Information

AI tools may help users understand lengthy texts by producing shorter summaries.

This can be useful when reviewing general educational information, public announcements, or non-sensitive documents.

A possible instruction is:

Summarise the following general information in five short points using simple language.

The trainer may provide a fictional or publicly available text for demonstration.

Participants should compare the summary with the original material and identify whether important information has been omitted or changed.

The exercise should emphasise that summaries are aids to understanding, not replacements for checking original documents when precise information is required.



Summarising Text with AI

2.2.5. AI for Translation and Language Assistance

AI-supported translation tools can help users understand information written in unfamiliar languages.

Potential applications include:

Co-funded by
the European Union

- Translating short messages.
- Understanding basic travel information.
- Explaining unfamiliar words.
- Preparing simple phrases for communication.
- Practising foreign-language vocabulary.

For example:

Translate the sentence “I would like information about the training programme” into Italian.

Participants may compare the generated translation with another reliable source or an available reference translation.

The trainer should explain that automated translations may contain errors, particularly when dealing with specialised terminology, legal documents, or ambiguous expressions.

Sensitive or confidential texts should not be entered into an AI service without appropriate consideration of privacy and data protection.



Translation with AI

2.2.6. AI for Personal Organisation

AI tools may help users organise activities and prepare simple plans.

Examples include:

- Preparing a weekly activity schedule.
- Creating a shopping list.
- Organising household tasks.
- Suggesting a structure for personal notes.
- Preparing a checklist for an event.
- Generating ideas for recreational activities.

A sample instruction is:

Co-funded by
the European Union

Prepare a simple weekly schedule that includes walking, reading, household activities, and time for learning basic computer skills.

The generated schedule should be treated as a suggestion that can be modified according to personal circumstances.

Participants should understand that AI does not automatically know their preferences, commitments, or individual needs.

2.2.7. AI for Travel and Everyday Planning

Artificial intelligence may assist with preliminary travel planning and information organisation.

For example, a user may request:

Suggest a simple checklist of things to prepare before a three-day trip.

The AI tool may provide a list of general preparations, such as checking travel documents, organising personal belongings, and reviewing transportation arrangements.

AI may also help generate questions that should be checked before travelling.

However, current transport schedules, ticket prices, entry requirements, and other time-sensitive information must be verified through appropriate official or reliable sources.

The programme should emphasise that AI-generated travel information may be incomplete or outdated.



Navigation and Travel

2.2.8. AI for Lifelong Learning

Artificial intelligence can support informal and structured learning by providing explanations, examples, and practice questions.

Co-funded by
the European Union

For adult learners, this may include:

- Understanding digital terminology.
- Reviewing basic computer concepts.
- Practising foreign-language phrases.
- Exploring historical or cultural topics.
- Generating simple educational exercises.
- Requesting additional explanations of unfamiliar subjects.

For example:

Explain what a PDF document is and how it differs from a photograph.

A learner may then ask:

Give me three simple questions to check whether I understood the explanation.

This interactive approach can support continued learning outside formal training sessions.

However, educational responses should be reviewed critically, particularly when they contain factual claims.

2.2.9. AI for Generating Ideas

AI tools may help users explore ideas for personal, educational, or community activities.

Examples include:

- Suggesting themes for a community event.
- Preparing ideas for a hobby.
- Creating a list of discussion questions.
- Developing a simple learning plan.
- Generating alternative ways to organise an activity.

A possible instruction is:

Suggest five simple activities for a community meeting where older adults can practise using smartphones.

The trainer may use this example to demonstrate how AI-generated ideas can be evaluated and adapted.

Participants should be encouraged to consider whether the suggestions are realistic, accessible, and appropriate for the intended audience.

Co-funded by
the European Union



Get Ideas with AI

2.2.10. AI and Accessibility Support

Some AI-supported technologies can improve access to digital information.

Potential functions include:

Speech-to-text

Converting spoken words into written text.

Text-to-speech

Reading digital text aloud.

Image description

Generating descriptions of visual content.

Automatic captions

Displaying text corresponding to spoken audio.

Language simplification

Rewriting complex explanations in more accessible language.

The availability and accuracy of these functions depend on the application and device.

Participants should understand that accessibility-related AI functions may make mistakes and should be used with appropriate awareness of their limitations.

2.2.11. Choosing Appropriate AI Tools

Not every AI application is suitable for every task.

Before using a tool, participants should consider:

1. What task do I want to complete?

Co-funded by
the European Union

2. Is this application suitable for the task?
3. Does it require an account?
4. Is the service free or paid?
5. What information will I need to enter?
6. Could the information be sensitive?
7. How can I verify the result?
8. Is there a simpler or more reliable alternative?

The trainer should explain that some applications may offer limited free access, paid subscriptions, or different functions depending on the account and service conditions.

Participants should not be encouraged to purchase subscriptions or disclose payment information as part of introductory training.

2.2.12. Reviewing AI-Generated Results

A central principle of practical AI literacy is that generated responses should be reviewed before use.

Participants should consider:

Accuracy

Does the response contain factual claims that need verification?

Relevance

Does it answer the original question?

Clarity

Is the information understandable?

Completeness

Are important details missing?

Appropriateness

Is the response suitable for the intended purpose?

Privacy

Does using the response involve unnecessary disclosure of personal information?

These questions should become part of participants' regular interaction with AI tools.

2.2.13. Practical Exercise: Preparing a Simple Email with AI

Learning objective: To use an AI tool to prepare and review a written message.

Required resources: Suitable AI application or trainer demonstration environment.

Instructions:

1. Open the selected AI tool.

Co-funded by
the European Union

2. Enter the following instruction:

"Write a short and polite email asking for information about a free digital skills course for adults."

3. Review the generated message.
4. Identify the greeting, main request, and closing.
5. Check whether the message includes any invented personal details.
6. Modify the text to make it clearer.
7. Discuss whether the final version is suitable for sending.

Expected learning result: The participant understands how AI can assist with writing while recognising the need for human review.

2.2.14. Practical Exercise: Simplifying Digital Terminology

Learning objective: To use AI for understanding unfamiliar digital concepts.

Instructions:

Participants select one of the following terms:

- Web browser.
- Digital password.
- Cloud storage.
- Online banking.
- Two-factor authentication.

They then ask an AI tool to explain the selected term in simple language.

The participant should:

1. Read the generated explanation.
2. Identify unfamiliar words.
3. Request clarification if necessary.
4. Compare the explanation with an appropriate educational source.
5. Explain the term in their own words.

Expected learning result: Improved ability to use AI as a learning aid while applying basic verification.

2.2.15. Practical Exercise: Creating a Personal Activity Plan

Learning objective: To explore AI as a tool for everyday organisation.

Instructions:

Participants use fictional or non-sensitive information to request a simple weekly activity plan.

Example instruction:

Co-funded by the European Union

Prepare a weekly plan for a fictional retired person who enjoys reading, walking, gardening, and learning to use a computer.

The participant reviews the generated plan and identifies:

- Useful suggestions.
- Activities that may need adjustment.
- Missing information.
- Ways to improve the original instruction.

The trainer encourages participants to modify the request and compare the results.

Expected learning result: The participant develops an understanding of how AI-generated suggestions can be adapted through additional instructions.

2.2.16. Practical Exercise: Comparing AI Responses

Learning objective: To recognise that different instructions may produce different results.

Activity description:

The trainer provides two instructions:

Instruction A:

Explain the internet.

Instruction B:

Explain what the internet is to an adult beginner using five short sentences and two everyday examples.

Participants compare the responses.

The trainer facilitates a discussion about clarity, relevance, and the importance of specifying the intended audience.

Expected learning result: Participants recognise that clear instructions can improve the usefulness of AI-generated responses.

2.2.17. Practical Exercise: Identifying Information

That Requires Verification

Learning objective: To develop critical awareness when using AI-generated information.

Activity description:

The trainer presents an AI-generated response containing several types of information, such as:

- A general explanation of a digital term.
- A claim about a current public service requirement.
- A suggested personal activity.
- A statement about a specific financial charge.

Co-funded by
the European Union

Participants identify which statements should be checked against official or reliable sources.

The trainer explains that time-sensitive, financial, legal, and other consequential information requires particular caution.

Expected learning result: Improved ability to distinguish between low-risk AI assistance and information requiring independent verification.

2.2.18. Learning Unit Summary

This learning unit introduces practical applications of artificial intelligence in everyday life.

Participants explore how AI tools can support writing, information simplification, translation, personal organisation, learning, and the generation of ideas.

Through guided exercises, learners develop familiarity with AI interaction and begin to understand the importance of clear instructions, human review, privacy, and independent verification.

The unit establishes a practical foundation for the subsequent learning activities on effective prompting, AI limitations, disinformation, and responsible digital behaviour.

2.3. Effective Interaction with AI Tools

2.3.1. Introduction to Effective AI Communication

One of the most important practical skills in using generative artificial intelligence is the ability to communicate instructions clearly.

Many AI applications allow users to interact through ordinary written or spoken language. This means that people do not necessarily need programming knowledge to use these tools.

However, the usefulness of an AI-generated response often depends on how the user formulates the request.

A general or unclear instruction may produce a response that is too broad, difficult to understand, or unrelated to the user's actual needs.

A more specific instruction can help the AI system generate a response that is better suited to the intended task.

This learning unit introduces practical techniques for communicating with AI tools effectively.

The objective is to help adult learners develop confidence in formulating requests, evaluating responses, and improving results through further interaction.

2.3.2. Understanding the Concept of a Prompt

A *prompt* is the instruction, question, or information provided by a user to an AI system.

A prompt may consist of a single sentence, a detailed description, or several related instructions.

Co-funded by the European Union

For example:

What is a web browser?

This is a simple prompt requesting an explanation.

A more detailed prompt might be:

Explain what a web browser is to a person aged 70 who has never used a computer. Use simple language and provide three everyday examples.

Both prompts address the same topic, but the second provides additional information about the intended audience and the desired response.

Participants should understand that a prompt does not need to contain technical terminology.

Clear everyday language is usually sufficient for introductory AI activities.

2.3.3. The Four Elements of a Useful Prompt

A practical introductory framework involves four elements.

1. The task

What should the AI tool do?

Examples include explaining, summarising, translating, comparing, organising, or drafting information.

2. The context

What background information is necessary to understand the request?

For example, the user may explain that the answer is intended for a beginner or for a community education activity.

3. The desired format

How should the answer be presented?

Possible formats include a short paragraph, numbered instructions, a checklist, or a simple table.

4. The level of detail

How detailed should the response be?

The user may request a brief explanation, a step-by-step guide, or several practical examples.

These elements can be combined into a simple formula:

Task + Context + Format + Level of Detail

For example:

Explain how to recognise a suspicious email. The explanation is intended for adults with limited digital experience. Present five practical warning signs in a numbered list and use simple language.

Co-funded by
the European Union

This structure can help learners formulate more useful requests.

2.3.4. Comparing Unclear and Clear Instructions

The trainer may use the following examples to demonstrate the importance of prompt clarity.

General instruction	More effective instruction
Explain computers.	Explain the three main functions of a computer to an adult beginner using simple language.
Write an email.	Write a polite email asking a community centre for information about computer courses.
Help me travel.	Prepare a general checklist for a fictional three-day trip, without including current prices or schedules.
Explain passwords.	Explain how to create a strong password and why passwords should not be shared.
Make a plan.	Prepare a simple five-day learning plan for an adult who wants to practise basic smartphone skills.

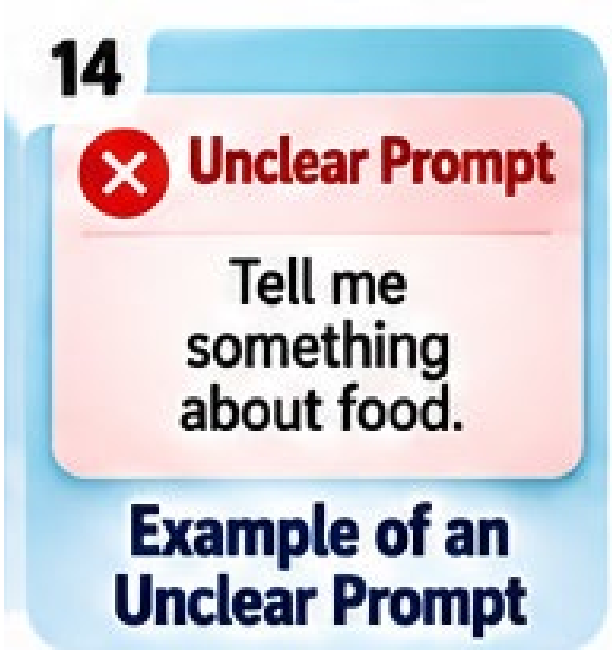
The trainer should explain that more detailed prompts do not automatically guarantee factual accuracy.

They can, however, help the system better understand the requested task and presentation.



Example of a Clear Prompt

Co-funded by the European Union



Example of an Unclear Prompt

2.3.5. Asking AI to Use Simple Language

Some AI-generated explanations may contain unfamiliar terminology or unnecessarily complex sentences.

Participants should learn that they can request a simpler explanation.

For example:

Explain this using everyday language.

Or:

Rewrite the explanation in five short sentences without technical terminology.

Another useful instruction is:

Give me an example from everyday life.

This approach is particularly relevant for older adults and learners with limited digital experience.

The trainer should encourage participants to ask additional questions whenever an explanation is unclear.

2.3.6. Requesting Step-by-Step Instructions

AI tools may be used to generate instructions for familiar digital tasks.

For example:

Explain step by step how to create a new folder on a Windows computer. Use short sentences and number each action.

Co-funded by the European Union

The generated instructions may provide a useful starting point.

However, participants should understand that software interfaces differ between devices and versions.

An AI-generated instruction may refer to a button or menu that is not present on the user's device.

When this happens, learners should avoid making uncertain changes to important settings and seek clarification or reliable assistance.

The trainer may demonstrate how to improve a request by specifying the operating system or application.

2.3.7. Providing Appropriate Context

Context helps an AI system adapt its response to the user's needs.

For example:

I am learning to use email for the first time. Explain how to attach a document using simple instructions.

This request provides relevant educational context without revealing sensitive personal information.

Participants should learn to distinguish between useful context and unnecessary personal data.

Appropriate context may include:

- The intended learning level.
- The type of task.
- The preferred language.
- The desired response format.
- The device or application being used.
- General preferences that are not sensitive.

Sensitive information such as passwords, identification numbers, banking credentials, or confidential documents should not be included in introductory AI exercises.

2.3.8. Improving an AI Response Through Follow-Up Questions

Effective AI interaction is often an iterative process.

A user may begin with a general question and then request clarification or improvement.

For example:

Initial request

Explain what cloud storage is.

Follow-up request

Co-funded by
the European Union

Explain it more simply.

Second follow-up

Give me an example involving photographs stored on a smartphone.

Third follow-up

What basic privacy precautions should I consider?

This sequence demonstrates how a conversation with an AI tool can support gradual learning.

Participants should understand that follow-up questions can improve relevance and clarity but do not guarantee accuracy.

2.3.9. Asking AI to Compare Alternatives

AI tools may help organise information into comparisons.

For example:

Compare email and instant messaging for everyday communication. Use a simple table with advantages and limitations.

The response may help learners understand differences between communication methods.

Another example is:

Compare a smartphone and a laptop for reading documents, writing emails, and participating in video calls.

Participants should review the comparison and consider whether it reflects their own needs.

For consequential decisions, factual claims should be checked against reliable sources.

2.3.10. Requesting Examples and Practice Questions

AI tools can support independent learning by generating exercises and examples.

A participant may ask:

Give me three simple practice questions about internet safety.

After answering, the learner may request:

Explain which answers are correct and why.

Alternatively:

Create a short fictional example of a suspicious email and ask me to identify the warning signs.

The trainer should explain that AI-generated educational exercises may contain errors and should be reviewed before use in formal assessment.

Co-funded by
the European Union

2.3.11. Recognising When a Prompt Is Too Broad

A prompt may be too broad when it asks for extensive information without defining the intended purpose.

For example:

Tell me everything about the internet.

Such a request may produce an unnecessarily long or unfocused response.

A more useful alternative is:

Explain the difference between the internet and a website in four short sentences.

Participants should practise dividing complex questions into smaller tasks.

This approach can improve understanding and reduce information overload.

2.3.12. Avoiding Unnecessary Personal Information

When preparing prompts, users should consider whether the requested task requires personal information.

For example, an AI tool can help prepare a general letter without receiving the user's full address, identification number, or other sensitive details.

A safer approach is to use placeholders.

Instead of entering real personal information, the user may write:

Prepare a formal letter using [Name], [Organisation] and [Date] as placeholders.

The participant can then complete the necessary information outside the AI tool.

This method supports privacy-conscious AI use.

2.3.13. Evaluating the Quality of an AI Response

After receiving a response, participants should assess its usefulness.

A simple evaluation checklist includes:

1. Does the response answer my question?
2. Is the explanation understandable?
3. Is the information relevant?
4. Are important details missing?
5. Does the response contain claims that require verification?
6. Is the suggested action safe and appropriate?

If the response is unclear, the user may request clarification.

If the response concerns important factual matters, it should be verified through reliable sources.

Co-funded by
the European Union

2.3.14. Practical Exercise: Improving a Prompt

Learning objective: To understand how clearer instructions can improve AI responses.

Instructions:

1. Enter the prompt: “Explain smartphones.”
2. Review the response.
3. Enter a revised prompt:

“Explain five basic smartphone functions to an adult beginner using simple language and everyday examples.”

4. Compare the two responses.
5. Identify which response is easier to understand.
6. Discuss how the additional instructions influenced the result.

Expected learning result: Participants recognise the value of specifying the task, audience, and desired format.

2.3.15. Practical Exercise: Learning Through Follow-Up Questions

Learning objective: To practise improving AI-generated explanations.

Instructions:

1. Ask an AI tool to explain what an email attachment is.
2. Read the explanation.
3. Request a simpler version.
4. Ask for a practical example.
5. Request three short questions to check understanding.
6. Compare the generated information with the trainer's demonstration.

Expected learning result: Participants become more confident in using follow-up questions to support learning.

2.3.16. Practical Exercise: Preparing a Structured Request

Learning objective: To apply the four-element prompt framework.

Scenario:

A fictional community organisation wants to prepare a simple invitation for an adult digital skills workshop.

Task:

Participants prepare a prompt that includes:

- The task: write an invitation.
- The context: an adult learning activity.
- The format: a short announcement.

Co-funded by
the European Union

- The level of detail: approximately 100 words.

A sample prompt is:

Write a short invitation of approximately 100 words for a fictional community workshop on basic digital skills for adults. Use friendly, accessible language and include placeholders for the date, time, and location.

Participants review the generated invitation and identify any information that requires correction or completion.

2.3.17. Learning Unit Summary

This learning unit introduces effective interaction with AI tools as a practical digital competence.

Participants learn to formulate clear prompts, provide appropriate context, request accessible explanations, and improve responses through follow-up questions.

They also develop awareness of privacy considerations and the need to evaluate AI-generated information.

The expected educational outcome is greater confidence in communicating with AI applications while maintaining independent judgement and responsible digital behaviour.

2.4. AI Limitations, Privacy and Responsible Use

2.4.1. Introduction to Responsible AI Use

Artificial intelligence can provide valuable assistance in communication, education, information processing, and personal organisation.

However, AI systems also have limitations that users must understand.

These limitations may involve factual accuracy, information completeness, privacy, bias, transparency, and the reliability of automated recommendations.

For adult learners, particularly those with limited digital experience, understanding these issues is essential for safe and informed participation in digital environments.

This learning unit introduces the principal risks associated with AI use and provides practical strategies for reducing them.

The objective is not to discourage the use of artificial intelligence but to support responsible and critical interaction with AI-supported technologies.

2.4.2. Understanding AI-Generated Errors

AI systems may generate information that is incorrect, incomplete, outdated, or inappropriate for the user's situation.

A response may appear clear and convincing even when it contains factual mistakes.

Co-funded by
the European Union

This can happen because generative AI systems produce responses through computational processes rather than through guaranteed verification of every statement.

Participants should understand that fluent language is not evidence of factual accuracy.

For example, an AI tool may provide an incorrect date, invent a source, or describe a procedure that does not exist.

Users should therefore evaluate AI-generated information according to the importance and potential consequences of the task.

2.4.3. What Are AI Hallucinations?

The term *AI hallucination* is commonly used to describe situations in which an AI system generates inaccurate, fabricated, or unsupported information and presents it as though it were factual.

Examples may include:

- Invented references to books or articles.
- Incorrect historical details.
- Non-existent legal provisions.
- Fabricated quotations.
- Incorrect information about public services.
- False claims about organisations or individuals.

For example, an AI tool might provide the name of a fictional government website when asked where to submit an administrative request.

A learner who relies on the response without verification may be misled.

The trainer should explain that hallucinations are a recognised limitation of generative AI and may occur even when the user provides a clear prompt.

2.4.4. Why AI Responses Require Verification

Verification means checking whether information is accurate and supported by reliable evidence.

The level of verification required depends on the nature of the information.

For example, an AI-generated suggestion for organising a fictional community activity may present relatively limited risk.

However, incorrect information about medical treatment, legal obligations, financial transactions, or official administrative procedures may have serious consequences.

Participants should be encouraged to use reliable sources when checking important claims.

Appropriate sources may include:

- Official public institution websites.
- Recognised educational institutions.

Co-funded by
the European Union

- Relevant professional organisations.
- Official service providers.
- Original documents and authoritative publications.

The trainer should emphasise that asking the same AI system whether its own response is correct does not constitute independent verification.



Check the Information!

2.4.5. Distinguishing Between Low-Risk and High-Risk AI Tasks

Different AI activities involve different levels of potential risk.

Type of task	Example	Recommended approach
Low-risk creative assistance	Generating ideas for a fictional community event	Review usefulness and suitability
General educational support	Explaining basic computer terminology	Compare with trusted learning materials
Information requiring accuracy	Describing current public service requirements	Verify through official sources
Financial information	Explaining banking fees or financial obligations	Check with official providers or qualified professionals
Health-related information	Explaining a medical term	Use reliable medical sources and consult qualified professionals for personal decisions
Legal information	Describing legal rights or administrative deadlines	Verify current law and obtain qualified advice when necessary

Co-funded by
the European Union

The purpose of this classification is to help participants understand that the consequences of an inaccurate response may differ significantly.

2.4.6. Personal Data and Artificial Intelligence

Personal data refers to information relating to an identified or identifiable individual.

Examples include:

- Names combined with identifying details.
- Home addresses.
- Telephone numbers.
- Email addresses.
- Personal identification numbers.
- Photographs identifying individuals.
- Financial information.
- Health-related information.

When using an AI application, information entered into the system may be processed according to the service provider's technical arrangements and privacy conditions.

The way data is stored, retained, or used differs between services and account settings.

Participants should therefore avoid assuming that every AI conversation is private or confidential.

Before sharing information, users should consider whether it is necessary for the task.



Privacy and Data Protection

2.4.7. Sensitive Information That Should Not Be Entered into AI Exercises

Introductory AI training should not require participants to enter sensitive or confidential information.

Co-funded by
the European Union

Examples include:

- Passwords.
- One-time authentication codes.
- Banking credentials.
- Payment card security information.
- Personal identification numbers.
- Confidential medical records.
- Private legal documents.
- Personal information about other individuals without an appropriate basis.
- Confidential organisational information.

The trainer should use fictional examples and demonstration materials whenever possible.

Participants should also understand that deleting a conversation from an application interface does not necessarily establish that all associated information has been immediately erased from every system.

Privacy and retention arrangements depend on the specific service.



Do Not Share Personal Data

2.4.8. Using Fictional Data and Placeholders

A practical way to reduce privacy risks is to replace real personal information with fictional data or placeholders.

For example, instead of entering an actual personal address, the user may write:

Prepare a general request for information using [Full Name] and [Address] as placeholders.

For educational exercises, participants may use fictional organisations, fictional participants, and invented contact details that are clearly designated for demonstration.

Co-funded by
the European Union

This approach allows learners to practise AI interaction without exposing unnecessary personal information.

2.4.9. Understanding AI Bias

AI systems may produce responses influenced by patterns, limitations, or imbalances in the data and methods used during their development.

This can result in biased or unfair representations.

Bias may affect how certain groups, professions, communities, or social situations are described.

For example, an AI-generated description of older adults might incorrectly assume that all older people have the same technological abilities.

The trainer should explain that such generalisations are inappropriate.

Participants should be encouraged to question responses that rely on stereotypes or present unsupported assumptions as facts.

2.4.10. AI and Stereotypes About Older Adults

Digital education should actively challenge the assumption that older adults are incapable of learning new technologies.

Learning ability and digital competence vary considerably between individuals.

Some older adults have extensive digital experience, while others may be encountering certain technologies for the first time.

AI-generated responses may occasionally reproduce oversimplified assumptions about age and technology.

Participants should understand that age alone does not determine a person's ability to acquire digital skills.

The programme promotes respectful, individualised, and inclusive approaches to technology education.

2.4.11. Understanding the Limits of AI Personalisation

AI tools may adapt their responses based on information provided by users or available through particular application features.

However, this does not mean that the system has complete knowledge of an individual's circumstances.

For example, an AI tool may suggest a weekly activity plan without knowing the user's actual commitments, accessibility needs, or preferences.

Co-funded by
the European Union

Participants should review personalised suggestions carefully and modify them where necessary.

Important personal decisions should not be delegated automatically to AI systems.

2.4.12. AI and Professional Advice

Artificial intelligence can explain general concepts and help users prepare questions for professionals.

However, AI-generated information should not be treated as a substitute for qualified professional advice in consequential matters.

Examples include:

Healthcare

AI may explain general medical terminology, but it cannot replace an appropriate medical examination or professional diagnosis.

Financial decisions

AI may explain financial concepts, but users should verify financial information through official providers and qualified advisers where appropriate.

Legal matters

AI may provide general explanations, but current legal requirements and individual circumstances should be checked through authoritative sources and qualified professionals.

Administrative procedures

AI may describe general steps, but official requirements, forms, and deadlines must be verified through the responsible institution.

This distinction supports informed use of AI while preserving human responsibility.

2.4.13. Transparency and Awareness of AI-Generated Content

Participants should understand the importance of recognising when content has been generated or substantially modified by artificial intelligence.

In some situations, transparency about AI use may be important for maintaining trust and avoiding misleading communication.

For example, a community organisation preparing informational materials with AI assistance should review the content and ensure that it does not contain inaccurate claims.

Where relevant, the organisation may also disclose that AI tools were used in preparing the material.

The exact obligations relating to disclosure depend on the context and applicable rules.

The general educational principle is that AI should not be used to deceive others about the origin, authenticity, or reliability of information.

Co-funded by
the European Union

2.4.14. Responsible Use of AI-Generated Images and Media

AI systems may generate realistic photographs, illustrations, voices, and videos.

Such content may be useful for educational or creative purposes.

However, realistic AI-generated media can also be misleading when presented as authentic evidence of events that did not occur.

Participants should understand that visual realism does not guarantee authenticity.

The trainer should introduce the importance of checking the source and context of unfamiliar images and videos.

These issues are explored in greater detail in the following learning unit on AI-generated disinformation and online fraud.



AI Image Generation

2.4.15. Recognising Manipulative AI-Based Services

Some online services may use exaggerated claims about artificial intelligence to attract users.

Examples include promises of guaranteed financial returns, effortless income, or access to supposedly exclusive AI systems.

Participants should be cautious when encountering offers that:

- Promise unrealistic results.
- Request immediate payment.
- Create artificial urgency.
- Require unnecessary personal information.
- Provide unclear information about the service provider.
- Use misleading testimonials or fabricated endorsements.

The trainer should explain that the presence of AI terminology does not establish the legitimacy or quality of a service.

Co-funded by
the European Union

2.4.16. Responsible Decision-Making Framework

The programme recommends a simple five-step framework for responsible AI use.

Step 1: Identify the purpose

What do I want the AI tool to help me accomplish?

Step 2: Consider privacy

Can I complete the task without entering sensitive information?

Step 3: Review the response

Does the answer appear relevant, understandable, and appropriate?

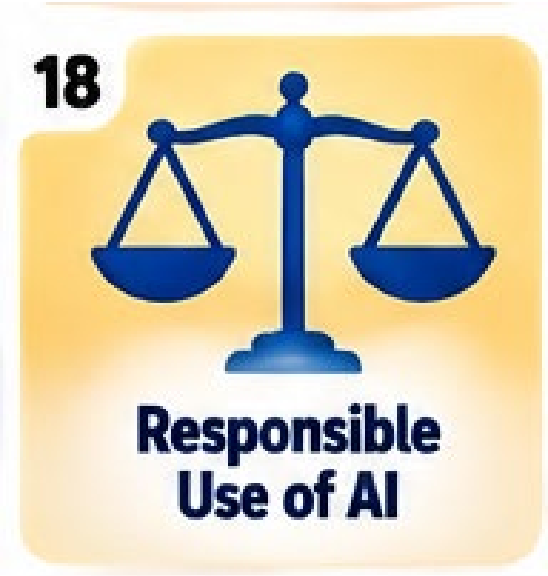
Step 4: Verify important information

Which factual claims require checking through reliable sources?

Step 5: Make an informed decision

Should I use, modify, reject, or seek further clarification about the generated result?

This framework can be applied across different AI applications.



Responsible Use of AI

2.4.17. Practical Exercise: Identifying AI Hallucinations

Learning objective: To recognise that AI-generated information may be inaccurate or fabricated.

Activity description:

The trainer prepares a fictional AI-generated response containing several factual statements.

Some statements are supported by reliable reference materials, while others are deliberately incorrect.

Co-funded by
the European Union

Participants are asked to:

1. Read the response.
2. Identify statements that require verification.
3. Compare the claims with the provided reference materials.
4. Mark statements that are inaccurate or unsupported.
5. Discuss why the original response may have appeared convincing.

Expected learning result: Participants develop awareness that confident wording does not guarantee factual accuracy.

2.4.18. Practical Exercise: Protecting Personal Information

Learning objective: To identify information that should not be entered into AI applications during introductory learning activities.

Instructions:

The trainer presents examples of information that a fictional user might consider entering into an AI tool.

Examples include:

- A general question about email.
- A fictional weekly schedule.
- A banking password.
- A sample invitation without personal details.
- A private medical report.
- A fictional description of a community event.
- A personal identification number.

Participants classify the examples according to whether they are appropriate for a basic AI training exercise.

The trainer discusses why certain information requires additional protection.

Expected learning result: Participants demonstrate improved awareness of privacy risks and the value of using fictional data.

2.4.19. Practical Exercise: Evaluating AI Advice

Learning objective: To distinguish between general AI assistance and information requiring professional or official verification.

Scenario:

A fictional participant asks an AI tool for help with several questions:

1. How can I organise my weekly activities?
2. What does the term “digital signature” mean?
3. What is the current deadline for a particular administrative procedure?

Co-funded by
the European Union

4. Should I change a prescribed medicine?
5. How can I write a polite email?

Participants discuss which tasks are suitable for general AI assistance and which require additional verification or professional guidance.

Expected learning result: Participants develop more informed judgement about the appropriate use of AI.

2.4.20. Practical Exercise: Responsible AI Decision-Making

Learning objective: To apply the five-step responsible AI framework.

Activity description:

Participants receive a fictional scenario involving an AI-generated response about a public service.

They should:

1. Identify the purpose of the original question.
2. Consider whether personal information was necessary.
3. Review the AI-generated response.
4. Identify claims requiring verification.
5. Explain how they would obtain reliable confirmation before taking action.

Expected learning result: Participants demonstrate a structured approach to responsible AI use.

2.4.21. Learning Unit Summary

This learning unit introduces the principal limitations and risks associated with artificial intelligence.

Participants learn that AI systems may generate inaccurate information, reproduce bias, and process user-provided data according to service-specific privacy arrangements.

The unit reinforces the importance of protecting personal information, verifying consequential claims, recognising manipulative services, and maintaining human responsibility for important decisions.

Through practical exercises, learners develop a more critical and informed approach to AI-supported technologies.

The expected educational outcome is greater confidence in using artificial intelligence responsibly, without excessive reliance on automated responses.

Co-funded by
the European Union

2.5. Artificial Intelligence, Disinformation and Online Fraud

2.5.1. Introduction to AI-Related Information Risks

Artificial intelligence has significantly expanded the possibilities for creating, modifying, and distributing digital content.

AI-supported technologies can generate written messages, photographs, audio recordings, and videos that may appear convincing to ordinary users.

These capabilities can support education, creativity, communication, and accessibility. However, they may also be misused to produce misleading information, impersonate individuals, manipulate public opinion, or facilitate online fraud.

For adults with limited digital experience, distinguishing authentic information from manipulated content may present particular challenges.

The objective of this learning unit is to strengthen learners' ability to recognise suspicious digital content, understand common AI-related fraud techniques, and apply practical verification strategies.

The programme adopts a balanced approach that promotes critical thinking without encouraging unnecessary fear or general distrust of digital technologies.

2.5.2. Understanding Misinformation and Disinformation

Online information may be inaccurate or misleading for different reasons.

Misinformation generally refers to false or inaccurate information shared without necessarily intending to deceive.

Disinformation refers to false or misleading information deliberately created or distributed to deceive or manipulate an audience.

Both can influence people's understanding of events, organisations, services, and social issues.

For example, an individual may unknowingly share an outdated announcement about a public service.

In another situation, a fraudulent website may deliberately publish false information to persuade visitors to provide personal details.

Artificial intelligence can make the production and distribution of misleading content easier and more scalable.

However, misinformation and disinformation also exist without AI involvement.

Co-funded by
the European Union



2.5.3. How Artificial Intelligence Can Be Used to Create Misleading Content

Generative AI tools can produce realistic-looking text, images, audio, and video.

These capabilities may be misused to create:

- Fabricated news articles.
- False statements attributed to public figures.
- Manipulated photographs.
- Synthetic voices imitating real individuals.
- Misleading videos.
- Fraudulent customer service messages.
- Fake product reviews.
- Impersonation attempts.
- Convincing phishing emails.

The trainer should explain that AI-generated content is not automatically fraudulent.

The relevant concern is whether the content is used deceptively, presented without appropriate context, or intended to manipulate the recipient.

2.5.4. Understanding Deepfakes

A *deepfake* is synthetic or manipulated media created using AI techniques to realistically imitate or alter a person's appearance, voice, or actions.

Deepfakes may involve:

Face manipulation

A person's face may be replaced or altered in a video or photograph.

Voice cloning

A synthetic voice may imitate the sound of a real person's voice.

Synthetic video

A video may be generated or manipulated to depict statements or events that did not occur.

Co-funded by
the European Union

Audio manipulation

An audio recording may be modified to create a misleading impression.

Some deepfake technologies have legitimate uses in creative production, accessibility, and entertainment.

However, deceptive deepfakes can be used for impersonation, reputational harm, financial fraud, and disinformation.

Participants should understand that realistic appearance or sound does not establish authenticity.



Deepfake (Fake Video)

2.5.5. Why Deepfakes Can Be Difficult to Recognise

Early manipulated media sometimes contained visible errors, such as unnatural facial movements or inconsistent lighting.

Modern synthetic media can be more convincing.

Although certain visual or audio irregularities may raise suspicion, their absence does not prove that content is authentic.

Potential warning signs may include:

- Unusual inconsistencies in facial movements.
- Audio that does not appear to match the context.
- Unexpected statements attributed to familiar individuals.
- Content presented without a verifiable source.
- Unusual requests accompanying a video or voice message.
- Claims designed to create urgency or emotional pressure.

The programme should emphasise that visual inspection alone is not a reliable method for identifying all deepfakes.

Co-funded by
the European Union

Verification of the source, context, and underlying claim is generally more important.

2.5.6. AI-Generated Images and False Visual Evidence

AI tools can generate realistic images depicting people, locations, objects, or events.

Such images may be useful for educational illustrations or creative activities.

However, they may also be presented misleadingly as photographs of real events.

For example, a fabricated image might appear to show damage to a public building, a fictional public gathering, or an event that never occurred.

Participants should learn to ask:

1. Who published the image?
2. Where did it originally appear?
3. Is the event described by reliable sources?
4. Is the image accompanied by verifiable information?
5. Could it have been generated or manipulated?
6. Is the image being presented outside its original context?

The trainer should explain that an authentic photograph can also be misleading if accompanied by a false description.

2.5.7. AI Voice Cloning and Impersonation Fraud

AI-supported voice synthesis can produce speech resembling the voice of a particular person.

This technology may be misused in impersonation scams.

For example, a person may receive a telephone call or voice message that appears to come from a relative requesting urgent financial assistance.

The voice may sound familiar, but this does not guarantee that the caller is the person they claim to be.

A fictional example may involve a caller saying:

I have an emergency and need you to transfer money immediately. Please do not call anyone else.

The trainer should explain that urgency, secrecy, and requests for immediate payment are important warning signs.

A safer response involves ending the suspicious interaction and contacting the person independently through a previously known and trusted communication channel.

Where appropriate, families may also establish simple verification arrangements for unexpected emergency requests.

Co-funded by
the European Union

2.5.8. AI-Enhanced Phishing Messages

Phishing is a form of fraud in which attackers attempt to obtain sensitive information or persuade individuals to perform unsafe actions.

AI tools may be used to create phishing messages with convincing language, appropriate formatting, and fewer obvious spelling mistakes.

Such messages may impersonate:

- Banks.
- Public institutions.
- Delivery companies.
- Online retailers.
- Telecommunications providers.
- Family members.
- Employers or community organisations.

Participants should understand that correct spelling and professional presentation do not guarantee legitimacy.

A suspicious message may request immediate action, personal information, authentication codes, or payment.

Users should verify unexpected requests independently rather than following unfamiliar links.



2.5.9. Fraudulent Investment and Financial Offers

Artificial intelligence may be used to create misleading financial advertisements, fabricated endorsements, or synthetic videos promoting fraudulent investment schemes.

Some advertisements may falsely suggest that a recognised person or organisation supports a particular financial product.

Common warning signs include:

- Promises of guaranteed profits.
- Claims of unusually high returns without risk.
- Pressure to invest immediately.

Co-funded by
the European Union

- Requests to transfer money through unfamiliar channels.
- Unverified endorsements.
- Unclear information about the service provider.

Participants should understand that AI-generated promotional materials may appear convincing while containing entirely fabricated claims.

Financial offers should be evaluated through reliable, independent sources and appropriate official information.

2.5.10. Fraudulent Online Shopping Content

AI-generated images, product descriptions, and reviews may be used to create convincing but deceptive online shopping offers.

A fraudulent website may display professional-looking photographs and positive customer testimonials without providing a legitimate product or service.

Learners should be encouraged to verify:

- The identity of the seller.
- The website address.
- Contact information.
- Payment arrangements.
- Consumer information.
- Independent reviews from credible sources.
- Whether the offer appears realistic.

Participants should not rely solely on attractive images or positive reviews when evaluating an unfamiliar retailer.

2.5.11. Manipulative Messages and Emotional Pressure

Fraudulent communication frequently relies on emotional manipulation.

Messages may attempt to create fear, excitement, sympathy, or urgency.

Examples include:

Fear

“Your account will be blocked immediately unless you confirm your information.”

Urgency

“You must act within the next ten minutes.”

Financial opportunity

“You have been selected for a guaranteed investment opportunity.”

Impersonation

“This is your relative. I need emergency financial assistance.”

Co-funded by
the European Union

Authority

“This message is from an official institution, and you must follow the instructions immediately.”

Participants should understand that emotional pressure is a reason to slow down and verify information.

2.5.12. A Practical Verification Method

The programme recommends a five-step verification method.

Step 1: Stop

Avoid responding immediately to unexpected or emotionally charged content.

Step 2: Identify the claim

Determine what the message, image, video, or recording is asking the user to believe or do.

Step 3: Check the source

Identify the original publisher or sender and consider whether the source is trustworthy.

Step 4: Verify independently

Use official websites, previously known contact details, or other reliable sources to confirm important information.

Step 5: Decide safely

Do not provide sensitive information, transfer money, or share questionable content until the relevant facts have been verified.

This method can be applied to suspicious emails, social media posts, telephone calls, videos, and online advertisements.



Verify Information

Co-funded by
the European Union

2.5.13. Using Search Engines for Verification

Search engines may help users investigate unfamiliar claims.

For example, if a suspicious message claims that a public institution has introduced a new mandatory payment, the user may search for the institution's official website and check whether the information is published there.

Participants should learn to avoid relying exclusively on the suspicious message itself.

The trainer may demonstrate how to:

1. Identify the main claim.
2. Search for the responsible institution.
3. Locate its official website.
4. Compare the claim with official information.
5. Seek further clarification through trusted contact channels when necessary.

Search results should also be evaluated critically because they may contain advertisements or misleading websites.

2.5.14. Understanding Reverse Image Search

Reverse image search is a technique that can help users find other online appearances of an image.

Depending on the available service, users may upload an image or provide an image reference to search for related results.

This may help identify whether an image appeared previously in another context.

For example, a photograph presented as evidence of a recent event may have been published several years earlier.

However, reverse image search does not automatically establish whether an image is authentic or AI-generated.

The absence of matching results is not proof that the image is genuine.

The trainer should demonstrate the technique using harmless, publicly available educational images.

2.5.15. Limitations of Automated AI-Detection Tools

Some online services claim to identify AI-generated images, text, audio, or video.

Such tools may provide useful indications in certain circumstances, but their results are not always reliable.

False positives and false negatives are possible.

Participants should understand that an automated detection result should not be treated as definitive proof.

Co-funded by
the European Union

A stronger verification approach combines source evaluation, contextual information, independent confirmation, and appropriate technical evidence where available.

2.5.16. Responsible Sharing of Digital Content

Digital communication makes it easy to distribute information quickly.

However, sharing inaccurate or misleading content can contribute to confusion, reputational harm, or financial risk.

Before forwarding a message or publishing content, participants should consider:

- Is the information verified?
- Is the original source identifiable?
- Could the content be misleading?
- Does it contain personal information about another individual?
- Could sharing it cause harm?
- Is it necessary to distribute the content?

The programme encourages responsible information sharing and respect for other people‘s privacy.



2.5.17. Responding to Suspected AI-Related Fraud

If a participant suspects that a message, call, or website is fraudulent, the following general precautions may be appropriate:

1. Stop interacting with the suspicious content.
2. Avoid opening unfamiliar links or attachments.
3. Do not disclose passwords or authentication codes.
4. Do not transfer money based solely on the suspicious request.
5. Verify the situation through an independent trusted channel.
6. Preserve relevant evidence when appropriate.
7. Contact the affected service provider or competent authority where necessary.

Co-funded by
the European Union

If sensitive credentials have already been disclosed, the individual should promptly contact the relevant provider through an official channel and follow appropriate account-protection procedures.

The exact response depends on the nature of the incident.



2.5.18. Practical Exercise: Recognising a Deepfake Scenario

Learning objective: To identify potential warning signs associated with synthetic media and impersonation.

Scenario:

A fictional participant receives a video message that appears to show a well-known public figure recommending an unfamiliar investment platform.

The video claims that users can obtain guaranteed profits by registering immediately.

Tasks:

Participants should:

1. Identify the main claim.
2. Recognise the financial promises.
3. Discuss whether the video could be manipulated.
4. Identify information requiring independent verification.
5. Explain why immediate registration would be inappropriate.
6. Describe a safer response.

Expected learning result: Participants demonstrate an understanding that realistic video content does not guarantee authenticity.

Co-funded by
the European Union

2.5.19. Practical Exercise: Voice Impersonation Fraud

Learning objective: To develop appropriate responses to suspicious voice messages.

Scenario:

A fictional older adult receives a voice message that sounds like a family member requesting an urgent money transfer.

The caller insists that the recipient must not contact anyone else.

Discussion questions:

1. Which elements of the message are suspicious?
2. Does recognising the voice prove the caller's identity?
3. How could the recipient verify the request?
4. Why is it important not to act under pressure?
5. What should the recipient do before transferring money?

Expected learning result: Participants identify independent identity verification as an essential precaution.

2.5.20. Practical Exercise: Evaluating an Online News Claim

Learning objective: To apply basic fact-checking methods.

Activity description:

The trainer presents a fictional online article containing an important claim about a public service.

Participants should:

1. Identify the source.
2. Check whether the article provides a publication date.
3. Identify the institution responsible for the service.
4. Locate an appropriate official information source.
5. Compare the claim with available verified information.
6. Explain whether further verification is necessary.

Expected learning result: Participants practise evaluating online claims without relying solely on the appearance of the content.

2.5.21. Practical Exercise: Identifying Manipulative Messages

Learning objective: To recognise emotional pressure and fraudulent communication techniques.

Activity description:

The trainer provides several fictional messages involving urgent payments, account warnings, unexpected prizes, and requests for personal information.

Co-funded by
the European Union

Participants identify the language used to create urgency, fear, or unrealistic expectations.

They then propose safer responses.

Expected learning result: Improved recognition of common manipulation techniques and more cautious digital decision-making.

2.5.22. Learning Unit Summary

This learning unit introduces the relationship between artificial intelligence, misleading information, and online fraud.

Participants learn about deepfakes, synthetic voices, manipulated images, AI-enhanced phishing, and fraudulent financial offers.

The unit emphasises source verification, critical thinking, privacy protection, and responsible information sharing.

Through realistic scenarios, learners develop practical strategies for responding to suspicious content and reducing the risk of digital deception.

2.6. Practical AI Exercises and Skills Assessment

2.6.1. Purpose of Practical Assessment

The practical assessment of Module 2 is designed to evaluate learners' ability to use artificial intelligence tools appropriately and critically.

The assessment focuses on practical competencies rather than advanced technical knowledge.

Participants are expected to demonstrate basic understanding of AI applications, formulate suitable instructions, review generated responses, and identify situations requiring verification.

The assessment should also establish whether participants understand essential privacy and cybersecurity precautions.

Individual progress and the level of assistance required should be considered throughout the process.

2.6.2. Assessment Objectives

The practical assessment seeks to determine whether participants can:

- Recognise common AI applications.
- Explain the basic purpose of generative AI.
- Formulate a clear prompt.
- Improve an instruction through additional context.
- Use AI for a simple everyday task.

Co-funded by
the European Union

- Review the usefulness of an AI-generated response.
- Identify information requiring independent verification.
- Recognise inappropriate disclosure of personal data.
- Understand the possibility of AI hallucinations.
- Identify common AI-related fraud scenarios.
- Apply safe decision-making principles.

2.6.3. Initial AI Knowledge Assessment

Before practical activities, the trainer may conduct a short introductory assessment.

Suggested questions include:

1. Have you previously used an AI application?
2. Can you identify an example of AI in everyday life?
3. Have you used automatic translation or a voice assistant?
4. Do you know what a prompt is?
5. Do you believe AI-generated answers are always correct?
6. Would you enter a banking password into an AI tool?
7. Have you heard of deepfake videos or synthetic voices?
8. Which AI application would you like to learn to use?

The purpose is to identify previous experience and adapt the training accordingly.

2.6.4. Practical Task 1: Recognising AI Applications

Objective: To assess understanding of common AI functions.

Task:

The trainer presents examples of digital activities.

Participants identify which may involve AI-supported functions and explain their reasoning.

Examples include:

- Automatic language translation.
- A basic calculator.
- AI-generated text.
- Voice recognition.
- A traditional text editor.
- AI-generated images.

Assessment focus:

Understanding of basic AI concepts and ability to recognise practical examples.

2.6.5. Practical Task 2: Creating a Clear Prompt

Objective: To assess the ability to formulate effective AI instructions.

Co-funded by
the European Union

Task:

Participants prepare a prompt requesting a simple explanation of a digital concept.

The prompt should specify:

1. The requested task.
2. The intended audience.
3. The desired format.
4. The level of detail.

Example:

Explain what an email attachment is to an adult beginner. Use simple language, three short steps, and one everyday example.

Assessment focus:

Clarity, relevance, and appropriate structure of the prompt.

2.6.6. Practical Task 3: Improving an AI Response

Objective: To assess the ability to refine AI interaction.

Task:

Participants enter an initial prompt and review the generated response.

They then prepare a follow-up instruction requesting greater clarity, additional examples, or a different format.

The participant compares the two responses and explains which is more useful.

Assessment focus:

Ability to identify limitations in an initial response and formulate appropriate follow-up instructions.

2.6.7. Practical Task 4: Using AI for Everyday Communication

Objective: To assess practical AI use in a familiar situation.

Scenario:

A fictional participant wishes to request information about an adult education course.

Task:

The learner should:

1. Open an appropriate AI application.
2. Request a draft email.
3. Review the generated text.
4. Identify any invented details.
5. Modify the message if necessary.

Co-funded by
the European Union

6. Explain why the message should be reviewed before sending.

Assessment focus:

Practical AI interaction, communication skills, and responsible review of generated content.

2.6.8. Practical Task 5: Identifying AI Hallucinations

Objective: To assess awareness of inaccurate AI-generated information.

Task:

The trainer provides an AI-style response containing several factual statements.

Some statements are intentionally inaccurate or unsupported.

Participants identify which claims require verification and use supplied reference materials to evaluate them.

Assessment focus:

Critical thinking, information verification, and understanding of AI limitations.

2.6.9. Practical Task 6: Protecting Personal Information

Objective: To assess privacy awareness.

Task:

Participants review examples of information that might be entered into an AI application.

They identify which examples are appropriate for a general educational exercise and which should be excluded or replaced with fictional data.

Assessment focus:

Recognition of sensitive information and ability to apply privacy-conscious practices.

2.6.10. Practical Task 7: Recognising AI-Related Fraud

Objective: To assess awareness of deepfakes and impersonation scams.

Scenario:

A fictional individual receives a voice message that appears to come from a relative requesting urgent financial assistance.

Task:

Participants should:

1. Identify suspicious characteristics.
2. Explain why the familiar voice is insufficient proof of identity.
3. Describe an independent verification method.
4. Identify actions that should be avoided.
5. Recommend a safe response.

Co-funded by
the European Union

Assessment focus:

Recognition of impersonation risks and appropriate protective behaviour.

2.6.11. Integrated Practical Scenario: Using AI Responsibly

Scenario title: Preparing Information for a Community Digital Skills Workshop

Learning objective: To combine practical AI use, critical thinking, and responsible information handling.

Scenario description:

A fictional community organisation plans to organise a short workshop introducing digital technologies to older adults.

A participant is asked to prepare a simple informational announcement with AI assistance.

Required activities:

1. Identify the purpose of the announcement.
2. Prepare a clear prompt.
3. Request an accessible text suitable for adult learners.
4. Review the generated announcement.
5. Identify missing or invented details.
6. Replace unverified information with placeholders.
7. Check whether the text contains inappropriate claims.
8. Prepare an improved final version.
9. Explain which parts required human review.
10. Describe the privacy precautions applied.

Expected learning result:

The participant demonstrates the ability to use AI as an assistance tool while maintaining responsibility for the final content.

2.6.12. Practical Assessment Criteria

The programme recommends evaluating performance through observable competencies.

Competence	Expected demonstration
Basic AI understanding	Explains AI in accessible language
Recognition of AI applications	Identifies familiar AI-supported functions
Prompt formulation	Creates a clear and relevant instruction
Response improvement	Uses follow-up instructions appropriately
Practical AI use	Completes a simple task using an AI tool

Co-funded by the European Union

Critical evaluation	Reviews generated content for accuracy and relevance
Information verification	Identifies claims requiring reliable confirmation
Privacy protection	Avoids unnecessary disclosure of sensitive information
Awareness of hallucinations	Recognises that AI may produce fabricated information
Fraud recognition	Identifies warning signs of AI-related deception
Responsible decision-making	Applies appropriate caution before acting

2.6.13. Levels of Achievement

The same three-level model introduced in Module 1 may be applied.

Level 1: Supported Performance

The participant completes AI-related tasks with step-by-step assistance.

Level 2: Partially Independent Performance

The participant performs most tasks independently but occasionally requires clarification or guidance.

Level 3: Independent Performance

The participant completes tasks independently, evaluates responses critically, and recognises relevant safety considerations.

These levels should be applied separately to each competence.

2.6.14. Trainer Assessment Checklist

Assessment item	Supported	Partially independent	Independent
Recognises common AI applications	☐	☐	☐
Understands the basic purpose of generative AI	☐	☐	☐
Creates a simple prompt	☐	☐	☐
Adds useful context to a prompt	☐	☐	☐
Requests clarification or improvement	☐	☐	☐
Uses AI for a simple everyday task	☐	☐	☐
Reviews an AI-generated response	☐	☐	☐
Identifies claims requiring verification	☐	☐	☐

Co-funded by the European Union

Recognises sensitive information	☐	☐	☐
Understands AI hallucinations	☐	☐	☐
Recognises potential deepfake fraud	☐	☐	☐
Applies basic responsible AI principles	☐	☐	☐

The checklist should be completed through observation and practical activities rather than solely through theoretical questioning.

2.6.15. Learner Self-Assessment

Participants may evaluate their own confidence using the following statements.

Statement	Not yet confident	Somewhat confident	Confident
I understand what artificial intelligence is	☐	☐	☐
I can recognise examples of AI in everyday life	☐	☐	☐
I can ask an AI tool a simple question	☐	☐	☐
I can prepare a clear instruction	☐	☐	☐
I can ask AI to simplify an explanation	☐	☐	☐
I can use AI to prepare a draft message	☐	☐	☐
I know that AI can produce incorrect information	☐	☐	☐
I understand the importance of verifying AI responses	☐	☐	☐
I know which personal information should not be shared	☐	☐	☐
I can recognise common warning signs of AI-related fraud	☐	☐	☐
I feel more confident using AI responsibly	☐	☐	☐

2.6.16. Reflection and Discussion

Following the practical assessment, participants should be encouraged to reflect on their experiences.

Co-funded by the European Union

Suggested discussion questions include:

1. Which AI application did you find most useful?
2. What difficulties did you experience when preparing prompts?
3. Did the AI tool provide any unclear or questionable information?
4. How did you decide whether the information was reliable?
5. Which privacy precautions did you apply?
6. What did you learn about deepfakes and AI-related fraud?
7. How could AI support your everyday activities?
8. Which skills would you like to develop further?

The discussion should support confidence-building and recognition of individual progress.

2.6.17. Trainer Feedback and Individual Recommendations

Trainer feedback should focus on demonstrated competencies and opportunities for further learning.

Recommendations may include:

- Additional practice in preparing prompts.
- Greater attention to reviewing AI-generated responses.
- Further exercises involving official information sources.
- Reinforcement of privacy precautions.
- Additional examples of fraudulent communication.
- Continued practice with accessible AI applications.

Feedback should recognise individual progress and avoid unrealistic expectations about the speed of learning.

2.6.18. Continued Independent Learning

Participants may be encouraged to continue practising AI-related skills through simple, low-risk activities.

Examples include:

- Asking AI to explain an unfamiliar digital term.
- Preparing a fictional invitation.
- Generating a checklist for a general activity.
- Comparing two explanations of the same concept.
- Requesting practice questions about digital literacy.
- Reviewing an AI-generated summary against its source text.

Participants should continue to avoid entering sensitive information and verify important factual claims independently.

Co-funded by
the European Union

2.6.19. Completion of Module 2

Module 2 provides adult learners with a practical introduction to artificial intelligence and its everyday applications.

The module combines basic conceptual understanding with direct interaction, critical evaluation, privacy awareness, and recognition of AI-related risks.

Completion should be assessed according to the learning activities undertaken and the competencies demonstrated by each participant.

The programme recognises that learners may progress at different speeds and require different levels of support.

The principal educational objective is not advanced technical proficiency but the ability to use AI-supported tools confidently, responsibly, and with appropriate human judgement.

2.6.20. Overall Module Conclusion

Artificial intelligence offers opportunities to support communication, learning, personal organisation, and access to information.

At the same time, its increasing capabilities create challenges associated with accuracy, privacy, disinformation, impersonation, and online fraud.

Module 2 addresses both dimensions through accessible explanations, practical activities, and structured assessment.

Participants are introduced to AI applications, effective prompting techniques, verification methods, and responsible decision-making principles.

The module promotes an understanding of artificial intelligence as a supportive technology rather than an unquestionable authority.

By strengthening practical AI literacy and critical awareness, the module contributes to the broader objectives of the Digital Era project and supports more informed participation in contemporary digital society.

MODULE 3: E-SERVICES AND DIGITAL PARTICIPATION

Module Overview

Digital services have become an increasingly important part of everyday life. Public institutions, financial organisations, healthcare providers, commercial businesses, and community organisations offer online services that can simplify access to information and reduce the need for physical visits.

However, the availability of digital services does not automatically guarantee that everyone can use them.

Co-funded by
the European Union

Adults with limited digital experience may encounter difficulties navigating online platforms, completing electronic forms, managing authentication procedures, and recognising legitimate service providers.

These difficulties can create barriers to accessing essential services and participating fully in contemporary society.

Module 3 introduces practical applications of digital technologies in public administration, financial services, online shopping, healthcare, social support, and community participation.

The module is designed to strengthen adult learners' ability to use electronic services independently while maintaining appropriate awareness of privacy, cybersecurity, and consumer protection.

Learning activities are based on realistic everyday situations and emphasise practical skills rather than advanced technical knowledge.

The module is organised into six learning units:

3.1. E-Government and Online Public Services
3.2. Online Banking and Financial Services
3.3. Online Shopping and Consumer Rights
3.4. Digital Health and Social Services
3.5. Digital Inclusion and Participation through Technology
3.6. Practical Exercises and Skills Assessment

Overall Learning Objective

To develop adult learners' ability to identify, access, and use appropriate electronic services safely and confidently, supporting greater independence, informed decision-making, and participation in everyday social and administrative activities.

Expected Learning Outcomes

By the end of the module, learners should be able to:

- Identify common categories of electronic services.
- Locate official public service websites.
- Understand the general purpose of digital identification and authentication.
- Navigate basic electronic forms.
- Recognise common online banking functions.
- Apply appropriate precautions when using financial services.
- Identify trustworthy online retailers.
- Understand basic consumer protection considerations.
- Locate appropriate digital health and social service information.
- Use digital technologies to support community participation.
- Recognise suspicious electronic service requests.

Co-funded by
the European Union

- Complete selected simulated digital service tasks with an appropriate level of independence.

3.1. E-Government and Online Public Services

3.1.1. Introduction to Electronic Government

Electronic government, commonly referred to as e-government, involves the use of digital technologies to provide public information, administrative procedures, and services to citizens and organisations.

Electronic public services may allow individuals to obtain information, submit requests, communicate with institutions, or access documents without visiting an administrative office in person.

For adult learners, these services may offer important practical benefits.

They can reduce travel requirements, save time, and improve access to information, particularly for individuals living in remote areas or experiencing mobility difficulties.

However, electronic services may also involve unfamiliar procedures, authentication requirements, and specialised terminology.

The objective of this learning unit is to introduce the basic principles of electronic public services and develop practical skills for accessing them responsibly.

3.1.2. Common Types of Electronic Public Services

Public institutions may provide a variety of electronic services.

Examples include:

Administrative information

Information about procedures, required documents, institutional responsibilities, and public service requirements.

Electronic applications

Online submission of certain requests, forms, or administrative applications.

Document verification

Checking the status or validity of certain documents where supported.

Appointments

Scheduling appointments with public institutions or service providers.

Electronic correspondence

Sending or receiving official communications through designated electronic systems.

Public information services

Accessing announcements, regulations, administrative guidance, and contact information.

The exact availability of these services depends on the country, institution, and relevant administrative system.

Co-funded by the European Union

Participants should understand that not every public service can be completed entirely online.



E-Government Services

3.1.3. Benefits of Electronic Public Services

Electronic public services may provide several advantages.

Time savings

Some administrative procedures can be initiated without visiting an office.

Improved accessibility

Online information may be available outside normal office hours.

Reduced travel

Digital access may be particularly useful for individuals living far from administrative centres.

Better information access

Official websites can provide guidance about procedures and requirements.

Document organisation

Electronic systems may allow users to download, store, and review certain documents.

Greater independence

Individuals may be able to complete routine administrative tasks with less reliance on assistance from others.

The trainer should also explain that digital services may not be equally accessible to all users and that alternative service channels may remain necessary.

3.1.4. Identifying Official Public Institution Websites

An essential competence is the ability to distinguish official institutional websites from unrelated or potentially fraudulent websites.

Co-funded by
the European Union

Participants should be encouraged to identify the institution responsible for the service before beginning an online procedure.

A practical approach includes:

1. Identifying the name of the responsible public institution.
2. Locating its official website through a reliable source.
3. Checking the website address carefully.
4. Reviewing the institution's contact information.
5. Finding the section dedicated to electronic services.
6. Confirming whether the intended service is available online.

The trainer should explain that fraudulent websites may imitate the appearance of legitimate public portals.

A secure connection is important, but HTTPS alone does not prove that a website is operated by an official institution.

3.1.5. Navigating an Electronic Service Portal

Electronic service portals commonly contain menus, categories, search functions, and instructions.

Although their design may vary, users often encounter similar interface elements.

These may include:

- Homepage.
- Service catalogue.
- Search function.
- User account area.
- Authentication options.
- Electronic forms.
- Instructions and guidance.
- Contact information.
- Help or support section.

Participants should practise locating relevant information within a demonstration portal or an appropriate official public website.

The trainer should explain that a user should read the service description and requirements before beginning an application.

3.1.6. Understanding Digital Identification

Some electronic services require users to confirm their identity before accessing personal information or completing an administrative procedure.

Digital identification refers to methods used to establish or verify a person's identity in an electronic environment.

Depending on the country and service, these methods may involve:

Co-funded by
the European Union

- Electronic identification systems.
- Digital identity applications.
- Electronic signatures.
- Authentication credentials.
- Additional verification procedures.

Participants should understand that identification requirements vary between services.

They should also recognise that accessing general public information may not require the same level of authentication as submitting an official application.



Digital ID and e-Signature

3.1.7. Understanding Electronic Signatures

An electronic signature is an electronic method used to sign or authenticate certain digital documents or transactions.

Different types of electronic signatures may have different legal effects and technical requirements.

The applicable rules depend on the jurisdiction and the particular administrative procedure.

Participants should understand the basic distinction between typing a name into a document and using an electronic signature method recognised for a specific official procedure.

The trainer should avoid presenting all electronic signature methods as legally interchangeable.

Learners should be encouraged to consult the instructions provided by the responsible institution.

Co-funded by
the European Union



Electronic Signature

3.1.8. Creating and Managing Online Service Accounts

Some public service platforms require a personal user account.

Account registration may involve:

1. Providing necessary registration information.
2. Creating appropriate authentication credentials.
3. Confirming contact details.
4. Completing identity verification where required.
5. Reviewing account settings.

Participants should understand the importance of protecting account credentials.

Passwords, authentication codes, and electronic identification credentials should not be shared with trainers or other participants.

Where possible, practical training should use demonstration accounts or simulated interfaces rather than participants' personal administrative accounts.

3.1.9. Completing Electronic Forms

Electronic forms allow users to enter information directly into a digital interface.

Common form elements include:

Text fields

Used to enter written information.

Selection menus

Used to choose from available options.

Checkboxes

Co-funded by
the European Union

Used to confirm or select particular statements.

Date fields

Used to enter dates in the required format.

Attachment functions

Used to upload supporting documents.

Submission controls

Used to send the completed form.

Participants should practise recognising these elements and understanding their purpose.

The trainer should explain that official forms may contain mandatory fields and specific formatting requirements.



Filling in Online Forms

3.1.10. Reviewing Information Before Submission

Submitting an electronic form may have administrative or legal consequences.

For this reason, users should carefully review the information before completing the submission.

A basic checklist includes:

1. Have I selected the correct service?
2. Have I read the instructions?
3. Have I completed the required fields?
4. Is the information accurate?
5. Have I attached the correct documents?
6. Do I understand what I am confirming?
7. Is the website authentic?

Co-funded by
the European Union

8. Am I ready to submit the information?

The programme should emphasise that learners should not submit real administrative applications during introductory exercises unless this is separately appropriate and intentionally authorised.

3.1.11. Uploading Documents to Electronic Portals

Some electronic services require users to upload supporting documents.

Common formats may include PDF documents and image files.

The trainer should demonstrate how to:

- Locate a document on the device.
- Check its file name.
- Identify the file format.
- Select the appropriate attachment function.
- Upload the document.
- Confirm that the correct file has been selected.

Participants should understand that uploading an incorrect document may delay or complicate an administrative procedure.

Exercises should use fictional documents containing no sensitive personal information.

3.1.12. Understanding Electronic Confirmations

After completing an electronic procedure, a service may provide a confirmation message, reference number, downloadable receipt, or other acknowledgement.

The type of confirmation depends on the particular service.

Participants should learn to recognise these confirmations and understand their possible importance.

Where appropriate, users may save the confirmation or reference number for future enquiries.

The trainer should explain that a technical submission confirmation does not necessarily mean that an administrative request has been approved.

3.1.13. Electronic Communication with Public Institutions

Some institutions allow users to communicate through official electronic channels.

Such communication may involve submitting enquiries, receiving notifications, or exchanging documents.

Participants should understand the importance of:

- Using the correct official communication channel.
- Providing relevant information.
- Avoiding unnecessary personal disclosures.
- Reviewing attachments.

Co-funded by
the European Union

- Keeping appropriate records.
- Checking whether additional action is required.

The trainer should explain that ordinary email and official electronic submission systems may have different procedural and legal functions.

3.1.14. Accessibility of Electronic Public Services

Electronic public services should be usable by people with diverse abilities and levels of digital competence.

However, some interfaces may remain difficult to navigate.

Potential accessibility barriers include:

- Small text.
- Complex menus.
- Unclear instructions.
- Limited compatibility with assistive technologies.
- Complicated authentication procedures.
- Short session time limits.
- Unfamiliar administrative terminology.

Trainers should demonstrate relevant accessibility features and provide step-by-step assistance.

Participants should be encouraged to seek official support or alternative access channels when an online service cannot be used effectively.

3.1.15. Common Risks When Using Electronic Public Services

Potential risks include:

Fraudulent websites

Websites that imitate official institutions.

Phishing messages

Messages requesting credentials or personal information under false pretences.

Incorrect submissions

Applications containing inaccurate or incomplete information.

Privacy exposure

Unnecessary disclosure of personal data.

Account compromise

Unauthorised access resulting from weak or disclosed authentication credentials.

Misleading information

Outdated or incorrect guidance presented by unofficial sources.

Co-funded by
the European Union

The programme encourages users to verify the source, review the procedure, and protect personal information.

3.1.16. Practical Exercise: Finding an Official Public Service

Learning objective: To develop the ability to locate reliable information about an electronic public service.

Required resources: Internet-connected device and an appropriate official website.

Instructions:

1. Identify a public service selected by the trainer.
2. Determine which institution is responsible.
3. Locate the institution‘s official website.
4. Find the electronic services section.
5. Identify the relevant service.
6. Read the service description.
7. Locate the available instructions.
8. Identify whether authentication or supporting documents are required.
9. Explain how the information was verified.

Expected learning result: The participant demonstrates the ability to navigate an official public service website and locate relevant procedural information.

3.1.17. Practical Exercise: Completing a Simulated Electronic Form

Learning objective: To develop confidence in completing basic electronic forms.

Required resources: Demonstration form containing fictional fields.

Instructions:

1. Open the demonstration form.
2. Read the instructions.
3. Enter fictional personal information.
4. Select the appropriate options.
5. Complete the required fields.
6. Attach a sample document if requested.
7. Review the completed form.
8. Identify any missing or incorrect information.
9. Discuss the submission procedure without sending a real administrative application.

Expected learning result: The participant demonstrates basic form completion skills and understands the importance of reviewing information before submission.

3.1.18. Practical Exercise: Recognising a Fraudulent Public Service Message

Learning objective: To identify suspicious electronic communication impersonating a public institution.

Scenario:

Co-funded by
the European Union

A fictional participant receives a message claiming that an official administrative account will be suspended unless personal identification information is entered immediately through an unfamiliar link.

Tasks:

Participants should:

1. Identify the main request.
2. Recognise the urgency used in the message.
3. Examine the apparent sender.
4. Explain why the link should not be trusted automatically.
5. Describe how to contact the institution independently.
6. Identify the information that should not be disclosed.

Expected learning result: Improved awareness of impersonation and phishing risks involving electronic public services.

3.1.19. Learning Unit Summary

This learning unit introduces the basic principles of electronic government and online public services.

Participants learn to locate official institutional websites, navigate electronic service portals, understand digital identification, complete simulated forms, and recognise electronic confirmations.

The unit also reinforces awareness of privacy, authentication, fraudulent websites, and responsible administrative communication.

The expected educational outcome is improved confidence and independence when accessing public information and appropriate electronic services.

3.2. Online Banking and Financial Services

3.2.1. Introduction to Digital Financial Services

Digital financial services allow individuals to access certain banking and payment functions through computers, smartphones, and other internet-connected devices.

These services may provide convenient ways to review account information, monitor transactions, make payments, and manage selected financial activities.

For adult learners, digital financial services can support independence and reduce the need for frequent visits to physical bank branches.

However, financial activities involve sensitive information and potentially significant consequences.

For this reason, introductory training should combine practical explanations with strong emphasis on cybersecurity, privacy, and responsible decision-making.

The purpose of this learning unit is to develop basic understanding of digital financial services without requiring participants to disclose financial information or perform real transactions.

Co-funded by
the European Union

3.2.2. Understanding Online Banking

Online banking refers to banking services accessed through an internet-connected interface.

Banks may provide these services through websites, mobile applications, or both.

Depending on the provider, available functions may include:

- Viewing account balances.
- Reviewing transaction histories.
- Checking payment information.
- Making transfers.
- Paying certain bills.
- Managing selected card settings.
- Receiving notifications.
- Communicating with customer support.

Not all banks offer identical functions.

Participants should be encouraged to consult their own bank's official information when they wish to use a particular service.



Online Banking

3.2.3. Understanding Mobile Banking Applications

A mobile banking application is software provided by a financial institution for use on a smartphone or tablet.

Such applications may allow users to access selected financial services without opening a web browser.

The trainer should explain the difference between a bank's official mobile application and an unrelated application that may imitate its appearance.

Co-funded by
the European Union

Participants should obtain banking applications only through appropriate trusted sources and verify the application publisher.

The exact installation and activation procedures depend on the bank.



Mobile Banking

3.2.4. Accessing a Banking Account Safely

Access to digital banking services generally requires authentication.

Authentication methods may include:

- Passwords.
- Personal identification codes.
- Biometric verification.
- One-time authentication codes.
- Banking authentication applications.
- Additional security confirmation procedures.

Participants should understand that authentication requirements are intended to protect access to financial information.

Passwords, banking PINs, one-time codes, and account recovery credentials should never be shared with trainers, strangers, or callers claiming to provide technical assistance.

3.2.5. Understanding Account Balances and Transactions

Digital banking interfaces commonly display account information.

An account balance generally indicates the amount recorded in an account, although available funds and displayed balances may differ depending on pending transactions and banking arrangements.

A transaction history may include:

- Incoming payments.

Co-funded by the European Union

- Outgoing transfers.
- Card payments.
- Fees.
- Other recorded account activities.

Participants should learn to recognise the general purpose of these sections.

Training exercises should use fictional account information and simulated transaction histories.

3.2.6. Understanding Bank Transfers

A bank transfer involves moving funds between accounts through a financial institution.

Depending on the service, a transfer may require information such as:

- Recipient name.
- Recipient account identifier.
- Transfer amount.
- Payment reference.
- Additional confirmation.

The exact required information and processing arrangements depend on the bank and transfer type.

Participants should understand that entering incorrect recipient details may lead to serious difficulties.

Before authorising any real payment, users should carefully review the recipient and transaction information.

Introductory training should use simulations rather than real transfers.

3.2.7. Understanding IBAN and Payment References

An International Bank Account Number, commonly called IBAN, is a standardised identifier used for bank accounts in many countries.

The format and length of an IBAN depend on the country.

Participants should understand that an IBAN identifies an account for payment purposes but does not, by itself, establish that the intended recipient is trustworthy.

A payment reference provides information about the purpose of a transfer.

The trainer may demonstrate how these fields appear in a fictional transfer form.

Participants should not use real personal banking details in classroom exercises.

3.2.8. Paying Bills Online

Some banks and payment service providers allow users to pay household or other bills electronically.

Examples may include:

- Electricity.

Co-funded by the European Union

- Water.
- Telecommunications.
- Internet services.
- Other recurring payments.

The available methods depend on the financial provider and the organisation receiving the payment.

Participants should understand the importance of verifying the bill, payment recipient, amount, and payment reference.

A familiar-looking payment request should not automatically be trusted, especially if it arrives unexpectedly through email or messaging applications.



Paying Bills Online

3.2.9. Understanding Payment Cards

Payment cards may be used for purchases in physical stores and online.

Different card types may have different functions and conditions.

Participants should become familiar with basic payment card terminology.

Card number

A number identifying the payment card.

Expiry date

The date indicating the card's validity period.

Card security code

A security feature used in certain payment processes.

PIN

Co-funded by
the European Union

A personal identification number used for certain card transactions or authentication procedures.

Participants should understand that card details are sensitive and must be protected.

The trainer should not request participants' real card numbers, PINs, or security codes.

3.2.10. Understanding Secure Online Payments

Online payments may involve entering payment information through a merchant's website or an authorised payment interface.

A secure payment process may include additional authentication or confirmation.

Participants should be encouraged to:

1. Verify the identity of the merchant.
2. Check the website address.
3. Review the payment amount.
4. Understand what they are purchasing.
5. Check whether the payment is one-time or recurring.
6. Review the available payment method.
7. Confirm the transaction only when satisfied that the information is correct.

The trainer should explain that a secure-looking website does not automatically guarantee that the merchant is legitimate.

3.2.11. Recognising Banking Phishing

Banking phishing involves fraudulent attempts to obtain financial credentials or persuade users to authorise unsafe transactions.

Common examples include messages claiming that:

- A bank account has been blocked.
- A payment requires immediate confirmation.
- A security update must be completed through a link.
- A suspicious transaction requires disclosure of an authentication code.
- A banking employee needs remote access to the user's device.

Participants should understand that scammers may imitate official logos, communication styles, and telephone numbers.

Unexpected requests should be verified through independently obtained official bank contact details.

3.2.12. Understanding Fraudulent Telephone Calls

Financial fraud may also involve telephone communication.

A caller may claim to represent a bank or another financial institution.

The caller may attempt to create fear by describing an alleged unauthorised transaction.

Participants should recognise warning signs such as:

Co-funded by
the European Union

- Requests for passwords or authentication codes.
- Instructions to transfer funds to a supposedly safe account.
- Pressure to act immediately.
- Requests to install remote-access software.
- Instructions not to contact the bank independently.

A safe response is to end the suspicious call and contact the bank through an official channel.

3.2.13. Remote-Access Fraud

Some scammers attempt to persuade individuals to install software that allows another person to control their computer or smartphone remotely.

Such software may have legitimate technical support uses, but it can also be misused.

Participants should understand that granting remote access to an unfamiliar person may expose sensitive information and financial accounts.

They should avoid installing remote-access applications at the request of unexpected callers or suspicious messages.

The trainer should explain this risk through fictional scenarios without demonstrating unsafe access to participants' personal devices.

3.2.14. Monitoring Financial Activity

Regularly reviewing financial activity may help users identify unexpected transactions or account changes.

Depending on the provider, digital banking services may offer transaction notifications and account alerts.

Participants should understand that notifications can be useful but should not replace careful review of account information.

If an unfamiliar transaction is identified, the individual should contact the relevant financial institution promptly through an official channel.

The appropriate response depends on the circumstances and the provider's procedures.

3.2.15. Using Shared and Public Devices

Financial services should be accessed with particular caution on shared or public computers.

Potential risks include:

- Stored authentication information.
- Unauthorised access.
- Malicious software.
- Exposure of account information.
- Failure to sign out.

Participants should generally avoid accessing sensitive banking services through unfamiliar or untrusted devices.

Co-funded by
the European Union

Where financial services are accessed on a personal device, appropriate device security and authentication measures should be maintained.

3.2.16. Accessibility and Digital Banking

Some adults may encounter difficulties using online banking because of unfamiliar terminology, small text, complex authentication procedures, or fear of making mistakes.

The trainer should provide explanations using simple language and visual demonstrations.

Relevant support strategies may include:

- Enlarging text where supported.
- Explaining interface terminology.
- Demonstrating navigation through fictional examples.
- Repeating essential procedures.
- Allowing sufficient practice time.
- Encouraging use of official bank support services.

Participants should not be pressured to activate online banking if they do not wish to use it.

Digital inclusion also involves respecting individual preferences and supporting access to appropriate alternative service channels.

3.2.17. Practical Exercise: Understanding a Simulated Banking Interface

Learning objective: To identify common online banking functions.

Required resources: Fictional banking interface or trainer-prepared screenshots.

Instructions:

1. Examine the demonstration banking interface.
2. Identify the account balance section.
3. Locate the transaction history.
4. Identify the transfer function.
5. Locate the security or account settings.
6. Identify the sign-out function.
7. Discuss which functions involve sensitive financial information.

Expected learning result: The participant develops familiarity with basic banking interface elements without accessing a real account.

3.2.18. Practical Exercise: Reviewing a Simulated Bank Transfer

Learning objective: To understand the information commonly required for a transfer and the importance of verification.

Scenario:

A fictional participant wishes to make a simulated payment to a fictional service provider.

The trainer supplies a sample transfer form containing fictional details.

Instructions:

Co-funded by
the European Union

1. Identify the recipient.
2. Review the account identifier.
3. Check the payment amount.
4. Review the payment reference.
5. Identify any missing or inconsistent information.
6. Explain which details should be checked before authorising a real transaction.

Important restriction: No real bank transfer or payment authorisation is performed.

Expected learning result: Improved understanding of payment verification and financial responsibility.

3.2.19. Practical Exercise: Recognising a Fraudulent Banking Message

Learning objective: To identify phishing and impersonation risks.

Scenario:

A fictional participant receives the following message:

“Your bank account has been suspended. Confirm your password and security code immediately using the link below.”

Tasks:

Participants should:

1. Identify the claimed sender.
2. Recognise the urgency.
3. Identify the request for sensitive information.
4. Explain why the link may be unsafe.
5. Describe an independent verification method.
6. Recommend an appropriate response.

Expected learning result: The participant demonstrates awareness of common banking phishing techniques.

3.2.20. Practical Exercise: Responding to a Suspicious

Telephone Call

Learning objective: To develop safe responses to financial impersonation attempts.

Scenario:

A caller claims to represent a bank and requests that the recipient install an application to prevent an alleged unauthorised payment.

Participants discuss:

1. Why the request is suspicious.
2. What risks may arise from installing unfamiliar software.
3. Why authentication credentials should not be disclosed.
4. How to contact the bank independently.
5. What actions should be avoided.

Co-funded by
the European Union

Expected learning result: Improved ability to recognise suspicious requests and respond appropriately.

3.2.21. Learning Unit Summary

This learning unit introduces the basic functions of online banking and digital financial services.

Participants develop an understanding of banking interfaces, account information, electronic transfers, online payments, and financial authentication.

The unit places particular emphasis on recognising phishing, impersonation, remote-access fraud, and unsafe payment requests.

Practical exercises use fictional information and simulated interfaces to avoid unnecessary financial or privacy risks.

The expected educational outcome is improved awareness of digital financial services and greater confidence in making informed, security-conscious decisions.

3.3. Online Shopping and Consumer Rights

3.3.1. Introduction to Online Shopping

Online shopping, also referred to as electronic commerce or e-commerce, allows consumers to purchase goods and services through websites, mobile applications, and other digital platforms.

Online shopping has become an important part of everyday economic activity. It provides access to a wide range of products and services, often without requiring consumers to visit physical stores.

For adult learners, particularly older adults and individuals living in rural or remote areas, online shopping may offer practical advantages.

These include greater product availability, easier price comparisons, home delivery, and access to services that may not be available locally.

However, online shopping also involves potential risks related to fraudulent retailers, misleading advertisements, unsafe payments, personal data protection, and consumer rights.

This learning unit introduces the basic principles of electronic commerce and develops practical skills for making informed and secure purchasing decisions.

The educational approach emphasises realistic scenarios, consumer awareness, and safe digital behaviour.

Co-funded by
the European Union



Online Shopping

3.3.2. Understanding Online Retailers and Marketplaces

Online shopping may take place through different types of digital platforms.

Online retailers

An online retailer sells goods or services directly through its website or application.

Online marketplaces

A marketplace provides a digital platform where different sellers may offer products or services.

Service booking platforms

These platforms allow users to reserve or purchase services, such as accommodation, transport, or educational activities.

Subscription services

Some platforms provide continuing access to digital content or services in exchange for recurring payments.

Participants should understand that the organisation operating a marketplace is not necessarily the seller of every product advertised on that platform.

The identity of the actual seller may be important when evaluating reliability and consumer rights.

3.3.3. Benefits of Online Shopping

Electronic commerce can provide several advantages.

Convenience

Consumers may browse products and place orders from home.

Product availability

Co-funded by
the European Union

Online platforms may offer products that are not available in nearby physical stores.

Price comparison

Consumers can compare prices and product characteristics across different retailers.

Access to information

Product descriptions, specifications, and consumer information may be available online.

Delivery options

Some retailers provide home delivery or collection services.

Accessibility

Online shopping may reduce travel requirements for individuals with mobility limitations.

The trainer should explain that these benefits depend on the reliability of the retailer and the conditions of the particular transaction.

3.3.4. Navigating an Online Store

Most online stores contain several common interface elements.

These may include:

- Product categories.
- Search functions.
- Product photographs.
- Product descriptions.
- Prices.
- Availability information.
- Shopping basket or cart.
- Delivery options.
- Payment options.
- Customer support information.
- Terms and conditions.

Participants should practise identifying these elements through a demonstration website or a simulated shopping interface.

The trainer should explain that adding an item to a shopping basket does not necessarily mean that a purchase has been completed.

3.3.5. Searching for Products

Online retailers commonly provide search functions that allow users to locate products using keywords.

For example, a participant may search for:

- Reading glasses.
- Household appliances.
- Gardening equipment.

Co-funded by
the European Union

- Books.
- Computer accessories.

Search results may be organised according to price, relevance, popularity, or other criteria.

Participants should understand that promoted products or sponsored listings may appear prominently.

The first product displayed is not necessarily the best or most suitable choice.

3.3.6. Understanding Product Descriptions

A product description may contain information about:

- Product characteristics.
- Size and dimensions.
- Materials.
- Technical specifications.
- Compatibility.
- Included accessories.
- Usage instructions.
- Warranty information.
- Delivery conditions.

Participants should learn to read product descriptions carefully before making a purchasing decision.

For example, when purchasing a smartphone accessory, compatibility with the intended device may be more important than the product's appearance.

The trainer should demonstrate how to identify essential information and distinguish it from promotional language.

3.3.7. Comparing Prices and Offers

Online shopping allows consumers to compare products offered by different retailers.

However, price comparison should consider more than the advertised product price.

Relevant factors may include:

- Delivery charges.
- Additional service fees.
- Payment conditions.
- Product specifications.
- Seller reliability.
- Return conditions.
- Warranty arrangements.
- Total purchase cost.

A product advertised at a lower price may ultimately cost more when additional charges are included.

Co-funded by
the European Union

Participants should practise comparing the total cost rather than relying exclusively on promotional prices.

3.3.8. Recognising Trustworthy Online Retailers

Before purchasing from an unfamiliar retailer, consumers should evaluate whether the seller appears legitimate.

Useful verification steps include:

1. Checking the website address.
2. Identifying the legal or commercial name of the seller.
3. Reviewing available contact information.
4. Examining delivery and payment conditions.
5. Reading return and cancellation information.
6. Looking for credible independent reviews.
7. Checking whether the offer appears realistic.
8. Avoiding pressure to complete a purchase immediately.

Participants should understand that professional website design and positive testimonials do not automatically establish trustworthiness.

Fraudulent retailers may imitate legitimate online stores.

3.3.9. Understanding the Shopping Basket

The shopping basket is a digital function used to collect products before completing an order.

Participants should learn how to:

- Add a product to the basket.
- Review selected products.
- Change quantities.
- Remove unwanted items.
- Check the total price.
- Review delivery charges.
- Continue to the checkout stage.

The trainer should emphasise the importance of reviewing the basket before confirming an order.

Practical activities should use a simulated store and avoid real purchases.

3.3.10. Understanding the Checkout Process

The checkout process is the stage at which a consumer reviews and confirms an online purchase.

Depending on the retailer, the process may involve:

1. Reviewing the shopping basket.
2. Providing delivery information.
3. Selecting a delivery method.

Co-funded by
the European Union

4. Choosing a payment method.
5. Reviewing the total cost.
6. Accepting applicable terms.
7. Confirming the order.

Participants should understand that a final confirmation may create a payment obligation.

The trainer should demonstrate how to recognise the final order confirmation stage.

3.3.11. Online Payment Methods

Online retailers may offer different payment methods.

Examples include:

- Payment cards.
- Bank transfers.
- Electronic payment services.
- Payment upon delivery, where available.
- Other authorised payment arrangements.

Each method may involve different procedures and protections.

Participants should be encouraged to use payment methods they understand and to review the relevant conditions.

They should avoid transferring money to unfamiliar recipients based solely on persuasive messages or unusually attractive offers.

3.3.12. Understanding Delivery Information

Online purchases may involve different delivery arrangements.

Relevant information may include:

- Estimated delivery period.
- Delivery address.
- Delivery charges.
- Available collection points.
- Tracking information.
- Procedures for reporting delivery problems.

Participants should understand that estimated delivery dates may change.

If a delivery does not arrive as expected, the consumer should contact the seller through an appropriate official communication channel.

Co-funded by
the European Union



Home Delivery

3.3.13. Understanding Consumer Rights in Online Shopping

Consumer protection rules may provide rights relating to information, delivery, withdrawal, defective goods, and contractual conditions.

Within the European Union, consumers purchasing from traders generally benefit from specific protections under applicable consumer legislation.

For many distance contracts, a 14-day withdrawal period applies, although important exceptions and conditions exist.

The applicable rights depend on factors such as the type of goods or services, the seller, the contractual arrangement, and the relevant legal framework.

Participants should understand that:

- Not every online transaction is subject to identical rules.
- Purchases from private individuals may be treated differently from purchases from traders.
- Certain products and services may be excluded from standard withdrawal rights.
- Consumer protections may differ when purchasing from sellers outside the European Union.

The trainer should encourage learners to consult official consumer protection information when evaluating a specific transaction.

Co-funded by
the European Union



Consumer Rights Online

3.3.14. Returning Products and Requesting Refunds

If a consumer wishes to return a product, the appropriate procedure depends on the circumstances and applicable consumer rights.

The process may involve:

1. Reviewing the seller's return information.
2. Identifying the applicable legal or contractual basis for the return.
3. Contacting the seller.
4. Following the required return procedure.
5. Keeping relevant correspondence.
6. Retaining proof of return where appropriate.
7. Monitoring the refund process.

Participants should understand that withdrawal from a distance contract and remedies for defective goods are different legal concepts.

The trainer should avoid suggesting that every online purchase can be returned under identical conditions.

3.3.15. Recognising Fraudulent Online Shops

Fraudulent online stores may attempt to obtain payments or personal information without delivering legitimate products.

Common warning signs include:

- Unrealistically low prices.
- Missing seller identification.
- Unclear contact information.
- Pressure to pay immediately.
- Suspicious website addresses.

Co-funded by
the European Union

- Unusual payment requests.
- Poorly explained delivery conditions.
- Misleading or fabricated customer reviews.

Participants should learn to consider several warning signs together.

The presence of a single unusual feature does not automatically prove fraud, but it may justify additional verification.

3.3.16. Online Shopping and Personal Data Protection

Online purchases commonly require some personal information.

Depending on the transaction, this may include:

- Recipient name.
- Delivery address.
- Contact information.
- Payment information.
- Order details.

Participants should understand that personal information should be provided only when necessary and through appropriate channels.

They should avoid saving payment credentials on unfamiliar devices and remain cautious about unexpected requests for additional information.

3.3.17. Recognising Fake Delivery Messages

Fraudulent messages may impersonate delivery companies and claim that a parcel cannot be delivered without additional payment or confirmation.

Such messages may contain links to deceptive websites.

Participants should understand that the existence of an expected delivery does not automatically make every delivery-related message legitimate.

When uncertain, users should check the order information through the retailer's official website or the delivery company's independently verified contact channels.

3.3.18. Practical Exercise: Comparing Online Products

Learning objective: To develop the ability to compare online offers.

Scenario:

A fictional participant wishes to purchase a basic household appliance.

The trainer provides three simulated product offers.

Tasks:

1. Identify the advertised price.
2. Review the product description.
3. Compare delivery charges.
4. Identify the total cost.

Co-funded by
the European Union

5. Review the seller information.
6. Compare the return conditions.
7. Select the offer that appears most appropriate.
8. Explain the reasons for the selection.

Expected learning result: Participants demonstrate the ability to compare products using relevant criteria rather than price alone.

3.3.19. Practical Exercise: Completing a Simulated Purchase

Learning objective: To understand the main stages of online ordering.

Instructions:

1. Open a simulated online store.
2. Search for a selected product.
3. Review the product description.
4. Add the item to the shopping basket.
5. Review the quantity and price.
6. Select a fictional delivery option.
7. Review the final order summary.
8. Identify the final confirmation stage.
9. Explain what should be checked before completing a real purchase.

Important restriction: No real payment or purchase is performed.

Expected learning result: The participant becomes familiar with the basic structure of an online transaction.

3.3.20. Practical Exercise: Identifying a Fraudulent Retailer

Learning objective: To recognise common indicators of online shopping fraud.

Scenario:

A fictional online store advertises expensive electronic equipment at an extremely low price.

The website provides no clear company information and requests immediate payment through an unfamiliar method.

Tasks:

Participants should identify:

- The unrealistic pricing.
- The absence of reliable seller information.
- The unusual payment request.
- The potential risks of immediate payment.
- Appropriate verification steps.

Expected learning result: Improved ability to recognise potentially fraudulent online offers.

3.3.21. Practical Exercise: Understanding a Consumer Complaint

Learning objective: To develop awareness of basic consumer protection procedures.

Co-funded by
the European Union

Scenario:

A fictional consumer receives a product that differs significantly from its advertised description.

Tasks:

1. Identify the problem.
2. Review the available order information.
3. Identify the seller.
4. Prepare a short complaint message.
5. Identify the evidence that may be relevant.
6. Discuss where official consumer guidance can be obtained.

Expected learning result: Participants understand the importance of documenting problems and using appropriate communication channels.

3.3.22. Learning Unit Summary

This learning unit introduces the main principles of electronic commerce and responsible online purchasing.

Participants learn to navigate online stores, compare products, understand ordering procedures, evaluate seller reliability, and recognise common fraud indicators.

The unit also introduces essential consumer protection concepts and the importance of reviewing payment, delivery, and return conditions.

Through simulated purchasing activities, learners develop practical confidence without being exposed to unnecessary financial risks.

3.4. Digital Health and Social Services

3.4.1. Introduction to Digital Health and Social Services

Digital technologies are increasingly used to provide access to healthcare information, medical appointments, administrative health services, and social support.

For adult learners, particularly older adults and individuals with mobility limitations, these services may offer important opportunities to access information and communicate with relevant institutions.

Digital health services may reduce certain administrative barriers and support more convenient interaction with healthcare providers.

However, healthcare and social service information often involves sensitive personal data.

The use of these services therefore requires particular attention to privacy, reliable information, authentication, and appropriate professional guidance.

This learning unit introduces the general functions of digital health and social services and develops practical skills for accessing them responsibly.

3.4.2. Understanding Digital Health Services

Co-funded by
the European Union

Digital health services involve the use of electronic technologies to support healthcare-related information, communication, and administrative activities.

Depending on the healthcare system and provider, services may include:

- Online appointment booking.
- Electronic prescriptions.
- Access to selected medical records.
- Digital communication with healthcare providers.
- Electronic referrals.
- Laboratory result access.
- Health-related administrative information.
- Telemedicine services.

The availability and requirements of these services vary between countries, institutions, and healthcare providers.

Participants should understand that digital health services complement, rather than automatically replace, in-person medical care.



Digital Health Services

3.4.3. Finding Reliable Health Information Online

The internet provides access to extensive health-related information.

However, not all online health content is accurate, current, or appropriate for individual circumstances.

Participants should be encouraged to use reliable sources, including:

- Official public health institutions.
- Recognised healthcare organisations.
- Licensed healthcare providers.
- Authoritative medical information services.

Co-funded by
the European Union

The trainer should explain that personal testimonials, advertisements, and social media posts should not automatically be treated as reliable medical evidence.

Information about symptoms, treatment, or medication should be interpreted with appropriate professional guidance.

3.4.4. Recognising Misleading Health Information

Misleading health content may include:

- Claims of guaranteed cures.
- Unsupported treatment recommendations.
- False statements about medication.
- Exaggerated product benefits.
- Fabricated professional endorsements.
- Misleading before-and-after photographs.
- AI-generated health advice presented as professional diagnosis.

Participants should learn to question information that promises immediate results or discourages consultation with qualified healthcare professionals.

The programme should emphasise that medical decisions must not be based solely on unverified online information.

3.4.5. Booking Medical Appointments Online

Some healthcare providers offer online appointment systems.

A typical appointment process may involve:

1. Accessing the provider's official website or application.
2. Locating the appointment section.
3. Selecting the relevant service.
4. Choosing an available appointment.
5. Providing the required information.
6. Reviewing the booking details.
7. Confirming the appointment.
8. Saving the confirmation where appropriate.

The exact process depends on the provider.

Practical training should use fictional booking information or a simulated interface.

Participants should not be required to disclose personal medical information.

Co-funded by
the European Union



3.4.6. Understanding Electronic Prescriptions

Electronic prescriptions allow authorised healthcare professionals to issue prescriptions through digital systems.

Depending on the national healthcare arrangements, patients may access prescription information or use designated identification procedures when obtaining prescribed medication.

Participants should understand that electronic prescriptions are part of regulated healthcare processes.

The trainer should explain the general concept without assuming that all countries or providers use identical systems.

Learners should be encouraged to follow the instructions provided by their healthcare professionals and official healthcare services.

3.4.7. Understanding Electronic Medical Records

Electronic medical records contain health-related information stored and managed in digital form.

Depending on the healthcare system, these records may include:

- Medical consultations.
- Diagnoses.
- Prescriptions.
- Laboratory results.
- Referrals.
- Other healthcare documentation.

Access to such information may require secure authentication.

Participants should understand that medical records contain sensitive personal data and should be handled carefully.

Co-funded by
the European Union

The trainer should use fictional examples rather than actual patient records.

3.4.8. Accessing Laboratory Results and Medical Documents

Some healthcare providers allow patients to access laboratory results or medical documents online.

A typical process may involve:

1. Accessing the provider's official platform.
2. Completing the required authentication.
3. Locating the relevant document section.
4. Identifying the available result.
5. Opening or downloading the document.
6. Saving it securely if necessary.

Participants should understand that laboratory results require appropriate medical interpretation.

A numerical result should not be interpreted as a diagnosis without relevant professional context.

3.4.9. Understanding Telemedicine

Telemedicine involves the provision of certain healthcare services through electronic communication technologies.

Depending on the healthcare provider and applicable rules, this may include video consultations, telephone consultations, or other forms of remote communication.

Potential benefits include:

- Reduced travel requirements.
- Easier communication with healthcare providers.
- Improved access in certain circumstances.
- Convenience for selected follow-up activities.

However, not every medical concern can be appropriately assessed remotely.

Participants should understand that telemedicine does not replace emergency medical care or necessary physical examinations.

Co-funded by
the European Union



Telemedicine (Online Consultation)

3.4.10. Preparing for a Digital Medical Consultation

When participating in an appropriate remote consultation, individuals may need to:

- Confirm the appointment through the official provider.
- Check their internet connection.
- Prepare the required device.
- Test microphone and camera functions.
- Choose a private location.
- Have relevant information available.
- Follow the provider's instructions.

Participants should understand the importance of maintaining privacy during medical communication.

Practical exercises should use fictional scenarios rather than real medical consultations.

3.4.11. Understanding Digital Social Services

Social services may provide assistance to individuals and families experiencing particular social, economic, or accessibility-related needs.

Digital social service platforms may provide information about:

- Available support programmes.
- Eligibility conditions.
- Application procedures.
- Required documentation.
- Contact information.
- Appointment arrangements.
- Administrative decisions or notifications.

The exact services depend on national and local administrative systems.

Co-funded by
the European Union

Participants should understand that online information can help them identify available services but does not automatically establish eligibility.



Social Services Online

3.4.12. Finding Information About Social Support

A practical approach to locating social service information includes:

1. Identifying the type of support required.
2. Determining the responsible public institution.
3. Locating its official website.
4. Reviewing the available services.
5. Reading the eligibility information.
6. Identifying required documents.
7. Checking the application procedure.
8. Contacting the institution for clarification when necessary.

The trainer should explain that eligibility rules and administrative requirements may change.

Official and current information should therefore be consulted.

3.4.13. Digital Services for Older Adults

Digital technologies may support older adults in accessing information and services related to everyday independence.

Potential applications include:

- Appointment scheduling.
- Communication with healthcare providers.
- Access to public service information.
- Social support enquiries.
- Educational activities.
- Community information.

Co-funded by
the European Union

- Communication with family members.
- Participation in online support groups.

The trainer should recognise that older adults have diverse digital abilities, preferences, and support needs.

The programme should avoid treating older people as a uniform group.

3.4.14. Accessibility and Assisted Digital Access

Some individuals may require assistance when accessing digital health or social services.

Potential barriers include:

- Visual impairments.
- Hearing difficulties.
- Limited digital experience.
- Complex authentication procedures.
- Difficult administrative terminology.
- Inaccessible website design.
- Limited internet connectivity.

Appropriate support may involve accessible interfaces, simplified instructions, individual guidance, or official assisted-service arrangements.

However, assistance should respect the individual's privacy and autonomy.

Trainers should not request passwords, authentication codes, or confidential medical information.

3.4.15. Protecting Health and Social Service Information

Health and social service information may include particularly sensitive personal details.

Participants should understand the importance of:

- Using official service platforms.
- Protecting authentication credentials.
- Avoiding unnecessary disclosure.
- Signing out of shared devices.
- Reviewing recipients before sending documents.
- Storing downloaded information appropriately.
- Being cautious about unexpected requests for medical or financial information.

The trainer should explain that sensitive documents should not be uploaded to unrelated AI tools or unfamiliar websites merely for convenience.

3.4.16. Recognising Fraudulent Health-Related Messages

Fraudulent messages may impersonate healthcare providers, pharmacies, public health institutions, or social service organisations.

Examples may include:

- False appointment confirmations.

Co-funded by the European Union

- Unexpected payment requests.
- Messages claiming that medical records must be verified immediately.
- Fraudulent offers of medical products.
- Requests for personal identification information.
- Links to imitation healthcare websites.

Participants should learn to verify unexpected communication through official contact channels.

3.4.17. AI and Online Health Information

Artificial intelligence may help users understand general medical terminology or prepare questions for healthcare professionals.

However, AI-generated health information may be incomplete, inaccurate, or unsuitable for an individual's circumstances.

Participants should understand that AI tools should not be used as a substitute for qualified medical assessment.

For example, an AI tool may help explain the general meaning of a medical term, but it should not determine whether a person should begin, stop, or change prescribed treatment.

The programme reinforces the importance of professional guidance for personal health decisions.

3.4.18. Practical Exercise: Finding a Healthcare Provider's Official Website

Learning objective: To develop the ability to locate reliable healthcare service information.

Instructions:

1. Identify a fictional healthcare information need.
2. Search for the relevant healthcare provider or public health institution.
3. Locate its official website.
4. Identify available contact information.
5. Find the appointment or service information section.
6. Review the instructions.
7. Explain how the source was verified.

Expected learning result: Improved ability to locate and evaluate official healthcare information.

3.4.19. Practical Exercise: Simulating an Online Appointment

Learning objective: To understand the general stages of online appointment booking.

Required resources: Trainer-prepared demonstration interface.

Instructions:

1. Open the simulated appointment platform.
2. Select a fictional healthcare service.
3. Review the available appointment options.

Co-funded by
the European Union

4. Choose a demonstration date and time.
5. Enter fictional contact details.
6. Review the booking summary.
7. Identify the confirmation stage.
8. Explain how the appointment information should be stored.

Important restriction: No real medical appointment is booked.

Expected learning result: The participant develops familiarity with basic appointment booking procedures.

3.4.20. Practical Exercise: Finding Social Service Information

Learning objective: To develop confidence in locating information about social support.

Scenario:

A fictional older adult wishes to obtain information about a community support service.

Tasks:

1. Identify the type of support.
2. Determine the responsible organisation or institution.
3. Locate an appropriate official information source.
4. Review the service description.
5. Identify the available contact channels.
6. Locate application information where relevant.
7. Explain which details require official confirmation.

Expected learning result: Improved ability to access relevant social service information.

3.4.21. Practical Exercise: Recognising Misleading Health Information

Learning objective: To develop critical awareness of online health claims.

Scenario:

A fictional website advertises a product claiming to cure numerous unrelated medical conditions immediately and without professional consultation.

Discussion questions:

1. Which claims appear unrealistic?
2. Is the information supported by reliable evidence?
3. Who is responsible for the website?
4. Does the content encourage avoidance of professional care?
5. Where could the claims be checked?
6. Why should personal medical decisions not rely on this advertisement?

Expected learning result: Participants recognise warning signs of misleading health information and the importance of qualified medical guidance.

3.4.22. Practical Exercise: Protecting Sensitive Health Information

Co-funded by
the European Union

Learning objective: To identify appropriate privacy practices when using digital health services.

Activity description:

The trainer presents fictional situations involving electronic medical documents, appointment confirmations, and requests for personal information.

Participants discuss:

- Whether the communication channel is appropriate.
- Which information is sensitive.
- Whether the recipient is correctly identified.
- Whether the requested disclosure is necessary.
- How the information could be protected.

Expected learning result: Improved awareness of privacy and responsible handling of health-related information.

3.4.23. Learning Unit Summary

This learning unit introduces the main functions of digital health and social services.

Participants develop familiarity with online appointment systems, electronic prescriptions, medical records, healthcare information, and digital access to social support.

The unit emphasises the importance of reliable sources, professional guidance, accessibility, and the protection of sensitive personal information.

Through practical simulations and realistic scenarios, learners strengthen their ability to access relevant services while recognising the limitations and risks associated with digital health information.

3.5. Digital Inclusion and Participation through Technology

3.5.1. Introduction to Digital Inclusion

Digital inclusion refers to the ability of individuals to access, understand, and use digital technologies in ways that support meaningful participation in everyday life.

It involves more than having access to a computer, smartphone, or internet connection.

Meaningful digital inclusion also requires appropriate skills, confidence, accessible services, and opportunities to use technology for personally relevant purposes.

For adults with limited digital experience, digital exclusion may create barriers to communication, education, employment, access to services, and participation in community activities.

These barriers may be particularly significant for older adults, people living in rural areas, individuals with disabilities, and people experiencing social or economic disadvantages.

The purpose of this learning unit is to demonstrate how digital technologies can support independence, social connections, lifelong learning, and active participation in society.

Co-funded by the European Union

3.5.2. Understanding Digital Exclusion

Digital exclusion occurs when individuals face barriers that prevent them from accessing or benefiting from digital technologies and services.

These barriers may include:

- Limited access to appropriate devices.
- Unreliable or unaffordable internet connectivity.
- Insufficient digital skills.
- Limited confidence in using technology.
- Accessibility difficulties.
- Language barriers.
- Lack of suitable training opportunities.
- Concerns about online security.
- Limited access to individual support.

Digital exclusion should not be understood simply as an individual's unwillingness to use technology.

It may result from a combination of personal, economic, technological, and social circumstances.

Training activities should therefore focus on reducing barriers rather than attributing difficulties to individual learners.

3.5.3. Digital Technologies and Personal Independence

Digital technologies can support independence by allowing individuals to complete everyday tasks with less reliance on assistance from others.

Examples include:

- Finding information about public services.
- Communicating with institutions.
- Organising personal activities.
- Accessing educational resources.
- Comparing products and services.
- Booking appointments.
- Maintaining communication with relatives.
- Participating in community initiatives.

For older adults, increased digital independence may contribute to greater confidence and autonomy.

However, the programme recognises that digital participation should remain a matter of informed personal choice.

Learners should not be pressured to use digital services when they prefer or require appropriate alternatives.

3.5.4. Maintaining Social Connections through Technology

Co-funded by
the European Union

Digital communication tools can help individuals maintain relationships with family members, friends, and community networks.

Common applications include:

Video calls

Allowing participants to communicate through live audio and video.

Messaging applications

Supporting the exchange of written messages, photographs, and other content.

Email

Providing a structured communication channel for personal and organisational correspondence.

Online groups

Creating opportunities for interaction around shared interests.

Digital invitations

Helping individuals receive information about social and community events.

The trainer should explain that online communication can complement face-to-face relationships.

Participants should also understand the importance of privacy settings, appropriate communication behaviour, and recognition of suspicious contacts.

3.5.5. Participating in Online Communities

Online communities bring together individuals who share interests, experiences, or common objectives.

Examples may include:

- Gardening groups.
- Book clubs.
- Cultural associations.
- Adult education communities.
- Local neighbourhood groups.
- Hobby-related forums.
- Community volunteering networks.

Participation may involve reading information, asking questions, exchanging experiences, or contributing to discussions.

Participants should learn to evaluate the credibility and purpose of online groups before joining.

They should also understand that public posts may be visible to a wider audience than originally expected.

Co-funded by
the European Union



Online Community and Participation

3.5.6. Understanding Social Media Participation

Social media platforms allow users to create, share, and interact with digital content.

Potential uses include:

- Maintaining social connections.
- Following community organisations.
- Learning about cultural events.
- Sharing educational information.
- Participating in discussions.
- Discovering local activities.

However, social media also presents risks involving misinformation, privacy exposure, impersonation, and unwanted contact.

The programme encourages learners to consider what information they share and who may be able to access it.

Participants should understand the distinction between private messages, restricted groups, and publicly visible posts.

3.5.7. Privacy in Online Communities

Online participation may involve sharing photographs, comments, personal experiences, or contact information.

Before publishing content, participants should consider:

1. Who can see the information?
2. Does the content identify another person?
3. Have relevant individuals agreed to the sharing of their information?
4. Could the content reveal sensitive personal details?
5. Is the platform appropriate for the intended communication?

Co-funded by
the European Union

6. Could the information be copied or distributed further?

The trainer should explain that deleting a post does not necessarily remove copies that other people may have saved or shared.

Practical exercises should use fictional profiles and demonstration content.

3.5.8. Digital Technologies and Lifelong Learning

Digital technologies provide opportunities for continued learning throughout adulthood.

Online educational resources may include:

- Recorded lessons.
- Educational videos.
- Digital books.
- Interactive exercises.
- Online courses.
- Language learning resources.
- Public educational platforms.
- Virtual lectures and workshops.

For adult learners, these resources may provide flexibility and opportunities to study at an individual pace.

However, the quality and reliability of online educational materials may vary.

Participants should learn to evaluate the source, purpose, and accessibility of educational content.



Online Learning

3.5.9. Identifying Appropriate Online Learning Opportunities

When considering an online learning activity, participants should review:

- The training provider.
- The learning objectives.

Co-funded by
the European Union

- The intended audience.
- The required digital skills.
- The course format.
- The language of instruction.
- Accessibility arrangements.
- Any participation fees.
- The type of certificate or confirmation offered.

The trainer should explain that not every online course provides a formally recognised qualification.

Learners should verify the status of any qualification or certificate when it is important for their personal or professional objectives.

3.5.10. Using Digital Cultural Resources

Digital technologies may improve access to cultural and educational experiences.

Examples include:

- Virtual museum exhibitions.
- Online library catalogues.
- Digital historical collections.
- Educational documentaries.
- Virtual cultural tours.
- Recorded public lectures.
- Online cultural events.

These resources can support lifelong learning and participation in cultural life.

For individuals with limited mobility or restricted travel opportunities, digital cultural resources may provide additional ways to explore educational and recreational interests.

The trainer should demonstrate how to locate appropriate resources from reliable cultural institutions.

3.5.11. Digital Participation in Community Activities

Community organisations increasingly use digital channels to communicate with members and the public.

These channels may provide information about:

- Local meetings.
- Educational activities.
- Volunteering opportunities.
- Cultural events.
- Community consultations.
- Public information campaigns.
- Social support initiatives.

Co-funded by
the European Union

Participants should learn to locate information from recognised organisations and verify the details of activities before participating.

Digital tools may help individuals become more informed about opportunities available in their communities.

3.5.12. Digital Civic Participation

Digital civic participation involves using electronic technologies to access public information, express opinions, engage with community issues, and participate in appropriate civic processes.

Examples may include:

- Reading public announcements.
- Accessing municipal information.
- Submitting enquiries.
- Participating in officially organised consultations.
- Following community initiatives.
- Communicating with public representatives.
- Learning about civic rights and responsibilities.

The availability of specific participation mechanisms depends on the relevant institutions and legal arrangements.

Participants should understand the difference between expressing an opinion on social media and participating through an official administrative or civic channel.

3.5.13. Recognising Reliable Community Information

Community information may circulate through official websites, social media groups, messaging applications, and informal networks.

Not all information is equally reliable.

Participants should practise identifying:

- The original source.
- The publication date.
- The organisation responsible.
- Relevant contact information.
- Whether the information is current.
- Whether the announcement is supported by an official source.

This competence is particularly important when information concerns public services, financial support, or community activities requiring registration or payment.

3.5.14. Digital Volunteering and Community Support

Digital technologies can support volunteering and community participation.

Potential activities include:

- Sharing information about community initiatives.

Co-funded by
the European Union

- Helping organise educational events.
- Supporting communication between volunteers.
- Participating in online awareness activities.
- Contributing to appropriate digital community resources.

The trainer should explain that volunteering opportunities should be evaluated carefully.

Participants should verify the organisation, understand the proposed activity, and avoid sharing unnecessary personal information.

3.5.15. Intergenerational Digital Learning

Intergenerational learning can provide opportunities for people of different ages to exchange knowledge and experiences.

Younger participants may be familiar with certain digital applications, while older participants may contribute valuable professional, social, and practical knowledge.

Effective intergenerational learning should be based on mutual respect.

The trainer should avoid assumptions that all younger people are digitally competent or that older adults necessarily require assistance.

Possible activities include:

- Joint exploration of digital cultural resources.
- Collaborative preparation of community announcements.
- Exchange of experiences about communication technologies.
- Discussion of online safety.
- Shared learning activities involving smartphones or computers.

Such activities may support social interaction and strengthen confidence.

3.5.16. Supporting Adults with Limited Digital Confidence

Some learners may experience uncertainty when participating in online communities or using unfamiliar digital services.

Appropriate support strategies include:

- Starting with familiar activities.
- Demonstrating one function at a time.
- Allowing repeated practice.
- Using accessible instructions.
- Encouraging questions.
- Providing individual assistance.
- Recognising progress.
- Respecting personal preferences.

The objective is to help participants develop confidence without creating unnecessary pressure.

3.5.17. Accessible Digital Participation

Co-funded by
the European Union

Digital inclusion requires attention to different accessibility needs.

Useful accessibility features may include:

- Adjustable text size.
- Screen readers.
- Voice input.
- Subtitles.
- High-contrast display options.
- Keyboard navigation.
- Simplified interfaces.

The availability and effectiveness of these features depend on the device, operating system, and application.

Participants should be encouraged to explore appropriate settings and request support when needed.

3.5.18. Balancing Online and Offline Participation

Digital technologies can create new opportunities for participation, but they should not be treated as a complete replacement for offline interaction.

Face-to-face communication, community meetings, printed information, and in-person services remain important.

The programme promotes a balanced approach in which digital tools complement existing forms of social participation.

Learners should be encouraged to select communication and participation methods that are appropriate for their circumstances.

3.5.19. Practical Exercise: Finding a Community Activity

Learning objective: To develop the ability to locate and verify information about community opportunities.

Scenario:

A fictional participant wishes to attend a local cultural or educational event.

Tasks:

1. Identify the type of activity.
2. Search for an appropriate organisation.
3. Locate its official website or verified communication channel.
4. Review the activity description.
5. Identify the date, location, and participation conditions.
6. Check whether registration is required.
7. Explain how the information was verified.

Expected learning result: Improved ability to locate community opportunities through digital channels.

Co-funded by
the European Union

3.5.20. Practical Exercise: Exploring an Online Cultural Resource

Learning objective: To use digital technologies for cultural participation and lifelong learning.

Instructions:

1. Open a recognised museum, library, or cultural institution's website.
2. Locate a digital exhibition or educational resource.
3. Explore the available content.
4. Identify the main topic.
5. Save or record the website address.
6. Explain how the resource could be used for independent learning.

Expected learning result: Greater familiarity with accessible digital cultural resources.

3.5.21. Practical Exercise: Preparing a Community Announcement

Learning objective: To apply digital communication skills in a community context.

Scenario:

A fictional community organisation plans an introductory digital skills workshop.

Tasks:

1. Prepare a short announcement.
2. Include the purpose of the activity.
3. Use fictional date and location details.
4. Review the clarity of the text.
5. Identify an appropriate digital communication channel.
6. Discuss privacy and responsible sharing.

Expected learning result: Improved ability to prepare accessible digital communication for community activities.

3.5.22. Practical Exercise: Safe Participation in an Online Group

Learning objective: To recognise appropriate online community behaviour and privacy precautions.

Scenario:

A fictional participant wishes to join an online group dedicated to gardening.

Tasks:

1. Identify the group's purpose.
2. Review its available rules.
3. Consider the visibility of posts.
4. Identify information that should remain private.
5. Recognise suspicious messages or requests.
6. Describe appropriate and respectful participation.

Expected learning result: Improved understanding of responsible online community participation.

Co-funded by
the European Union

3.5.23. Learning Unit Summary

This learning unit explores how digital technologies can support social inclusion, lifelong learning, community engagement, and personal independence.

Participants learn to identify online communities, educational resources, cultural opportunities, and appropriate channels for civic participation.

The unit also addresses privacy, accessibility, reliable information, and respectful digital communication.

Through practical exercises, learners strengthen their ability to use technology for meaningful participation in everyday social and community activities.

3.6. Practical Exercises and Skills Assessment

3.6.1. Purpose of the Assessment

The practical assessment of Module 3 is designed to evaluate participants' ability to access, understand, and use selected electronic services.

The assessment focuses on realistic everyday tasks involving public services, financial information, online shopping, healthcare, social support, and community participation.

The purpose is not to test advanced technical knowledge or require learners to complete real financial or administrative transactions.

Instead, the assessment examines practical digital competence, awareness of relevant risks, and the ability to make informed decisions.

The assessment should recognise individual progress and allow appropriate support for participants with different levels of digital experience.

3.6.2. Assessment Objectives

The assessment seeks to determine whether participants can:

- Locate an official electronic service website.
- Identify relevant service information.
- Navigate basic electronic forms.
- Recognise authentication requirements.
- Understand common online banking functions.
- Identify suspicious financial messages.
- Compare online shopping offers.
- Recognise basic consumer protection considerations.
- Locate appropriate digital health information.
- Find information about social support.
- Identify online community opportunities.
- Apply relevant privacy and cybersecurity precautions.

3.6.3. Initial Digital Services Assessment

Co-funded by
the European Union

Before beginning practical tasks, the trainer may ask participants about their previous experience with electronic services.

Suggested questions include:

1. Have you previously used an online public service?
2. Can you identify an official institutional website?
3. Have you completed an electronic form?
4. Are you familiar with online banking?
5. Have you purchased a product online?
6. Do you know how to recognise a suspicious payment request?
7. Have you booked an appointment online?
8. Have you used an online cultural or educational resource?
9. Do you participate in online community groups?
10. Which digital service would you most like to learn to use?

The answers may help the trainer identify relevant learning needs.

3.6.4. Practical Task 1: Finding an Official Electronic Service

Objective: To assess the ability to locate and evaluate official public service information.

Task:

Participants are asked to find information about a selected administrative service.

They should:

1. Identify the responsible institution.
2. Locate its official website.
3. Find the relevant service.
4. Review the available instructions.
5. Identify whether authentication is required.
6. Explain how the website's authenticity was evaluated.

Assessment focus: Navigation, information retrieval, and source verification.

3.6.5. Practical Task 2: Completing a Simulated Electronic Form

Objective: To assess basic form completion skills.

Task:

Participants complete a fictional electronic form using sample information.

They should:

1. Read the instructions.
2. Identify mandatory fields.
3. Enter appropriate fictional information.
4. Select relevant options.
5. Review the completed form.
6. Identify any errors.

Co-funded by
the European Union

7. Explain the purpose of the submission stage.

Assessment focus: Accuracy, attention to instructions, and responsible review.

3.6.6. Practical Task 3: Understanding a Digital Banking Interface

Objective: To assess familiarity with common online banking functions.

Task:

Participants examine a simulated banking interface.

They identify:

- Account balance.
- Transaction history.
- Payment functions.
- Security settings.
- Sign-out function.

They should also explain why financial authentication credentials must remain confidential.

Assessment focus: Functional understanding and financial security awareness.

3.6.7. Practical Task 4: Identifying a Suspicious Financial Request

Objective: To assess recognition of financial fraud indicators.

Scenario:

A fictional participant receives an unexpected message requesting immediate confirmation of banking credentials.

Task:

Participants identify:

1. The suspicious request.
2. The use of urgency.
3. The sensitive information involved.
4. The risks of following the message.
5. An appropriate independent verification method.

Assessment focus: Fraud awareness and safe decision-making.

3.6.8. Practical Task 5: Comparing Online Shopping Offers

Objective: To assess responsible consumer decision-making.

Task:

Participants compare two or three fictional product offers.

They should evaluate:

- Product description.
- Advertised price.
- Delivery costs.

Co-funded by the European Union

- Total cost.
- Seller information.
- Payment conditions.
- Return information.

Participants explain which offer they would select and why.

Assessment focus: Comparison skills, consumer awareness, and recognition of potential risks.

3.6.9. Practical Task 6: Understanding an Online Appointment

Objective: To assess familiarity with digital appointment procedures.

Task:

Participants use a simulated appointment interface.

They should:

1. Identify the service.
2. Select an available demonstration appointment.
3. Enter fictional contact information.
4. Review the booking summary.
5. Identify the confirmation stage.
6. Explain how appointment information should be stored.

Assessment focus: Navigation, procedural understanding, and privacy awareness.

3.6.10. Practical Task 7: Finding Social Support Information

Objective: To assess the ability to locate relevant social service information.

Scenario:

A fictional individual wishes to obtain information about an available community support service.

Task:

Participants identify the responsible organisation, locate appropriate information, review the service description, and identify contact options.

They should explain which details require official confirmation.

Assessment focus: Information searches, source evaluation, and understanding of service access.

3.6.11. Practical Task 8: Identifying a Community

Participation Opportunity

Objective: To assess the ability to use digital technologies for social and cultural participation.

Task:

Participants locate an appropriate educational, cultural, or community activity.

They should identify:

Co-funded by
the European Union

- The organising institution.
- The purpose of the activity.
- Participation requirements.
- Relevant contact information.
- Any registration procedure.
- The reliability of the information source.

Assessment focus: Independent information retrieval and meaningful digital participation.

3.6.12. Integrated Practical Scenario: Planning a Digitally

Supported Week

Scenario title: Everyday Digital Independence

Learning objective: To combine skills from the three learning modules in a realistic, integrated activity.

Scenario description:

A fictional adult learner wishes to organise several everyday activities using digital technologies.

The activities include:

- Finding information about an electronic public service.
- Preparing a general enquiry email.
- Reviewing a fictional online shopping offer.
- Identifying how to book a medical appointment.
- Finding an educational or cultural activity.
- Using an AI tool to prepare a simple weekly checklist.

Required tasks:

Task A: Public service information

Locate an appropriate official public service website and identify the relevant information.

Task B: Digital communication

Prepare a polite enquiry email using fictional details.

Task C: Consumer decision-making

Compare two simulated online shopping offers and identify the safer or more appropriate option.

Task D: Digital health service

Explain how to locate an official healthcare provider's appointment information.

Task E: Community participation

Identify a suitable online educational or cultural resource.

Task F: AI-supported organisation

Co-funded by
the European Union

Use an AI tool to prepare a simple weekly activity checklist.

Task G: Safety review

Identify privacy, cybersecurity, and information verification considerations associated with the activities.

Expected learning result:

The participant demonstrates the ability to combine basic digital skills, AI-supported assistance, and electronic service awareness in everyday situations.

3.6.13. Practical Assessment Criteria

Competence	Expected demonstration
Official service identification	Locates a relevant institutional website
Website navigation	Finds appropriate information and instructions
Electronic form completion	Completes a simulated form accurately
Authentication awareness	Recognises the importance of secure identification
Banking awareness	Identifies basic financial service functions
Financial fraud recognition	Recognises suspicious requests
Online shopping competence	Compares offers and evaluates seller information
Consumer awareness	Recognises relevant purchase and return considerations
Digital health awareness	Locates appropriate healthcare service information
Social service access	Identifies relevant information and contact channels
Community participation	Finds suitable digital participation opportunities
AI-supported organisation	Uses AI appropriately for a simple planning task
Privacy protection	Avoids unnecessary disclosure of personal information
Critical evaluation	Verifies important information through reliable sources

3.6.14. Levels of Achievement

The programme applies the same three-level assessment approach used in Modules 1 and 2.

Level 1: Supported Performance

The participant completes tasks with substantial trainer guidance.

Level 2: Partially Independent Performance

The participant completes most tasks independently but requires occasional assistance.

Level 3: Independent Performance

Co-funded by the European Union

The participant completes tasks independently, evaluates information appropriately, and applies relevant safety precautions.

These levels should be used to recognise individual progress rather than to create unnecessary competition between learners.

3.6.15. Trainer Assessment Checklist

Assessment item	Supported	Partially independent	Independent
Locates an official public service website	☐	☐	☐
Navigates electronic service information	☐	☐	☐
Completes a simulated electronic form	☐	☐	☐
Understands basic authentication requirements	☐	☐	☐
Identifies common online banking functions	☐	☐	☐
Recognises suspicious financial requests	☐	☐	☐
Compares online shopping offers	☐	☐	☐
Understands basic consumer rights considerations	☐	☐	☐
Locates digital health service information	☐	☐	☐
Finds relevant social service information	☐	☐	☐
Identifies digital community opportunities	☐	☐	☐
Applies privacy precautions	☐	☐	☐
Verifies important information	☐	☐	☐
Completes an integrated digital task	☐	☐	☐

3.6.16. Learner Self-Assessment

Participants may complete the following self-assessment after the practical activities.

Statement	Not yet confident	Somewhat confident	Confident
I can find an official public institution website	☐	☐	☐

Co-funded by the European Union

I can locate information about an electronic service	☐	☐	☐
I understand the basic structure of an electronic form	☐	☐	☐
I know why digital identification must be protected	☐	☐	☐
I understand the basic functions of online banking	☐	☐	☐
I can recognise suspicious financial messages	☐	☐	☐
I can compare products in online stores	☐	☐	☐
I know that online consumers may have specific rights	☐	☐	☐
I can find healthcare service information online	☐	☐	☐
I can locate information about social support	☐	☐	☐
I can find online educational or cultural activities	☐	☐	☐
I understand the importance of protecting personal information	☐	☐	☐
I feel more confident using electronic services	☐	☐	☐

3.6.17. Individual Reflection

After completing the practical tasks, participants should be encouraged to reflect on their learning experiences.

Suggested questions include:

1. Which electronic service was easiest to understand?
2. Which activity was most challenging?
3. Did you encounter unfamiliar terminology?
4. What helped you complete the practical tasks?
5. Which digital service would be most useful in your everyday life?
6. What did you learn about protecting personal information?
7. How can you recognise suspicious electronic service requests?
8. Which skills would you like to practise further?

The trainer should provide opportunities for participants to discuss their experiences without pressure or negative judgement.

3.6.18. Trainer Feedback

Co-funded by the European Union

Trainer feedback should be based on observable performance.

Feedback may address:

- Ability to navigate websites.
- Accuracy in completing simulated forms.
- Understanding of financial security.
- Consumer awareness.
- Information verification.
- Privacy protection.
- Independent problem-solving.
- Confidence in using digital services.

Recommendations should be practical and adapted to the learner's individual needs.

3.6.19. Continued Independent Practice

Following the training, participants may continue developing their skills through appropriate low-risk activities.

Examples include:

- Visiting an official public institution website.
- Reading information about a public service.
- Exploring a recognised online museum.
- Comparing general product information.
- Reviewing consumer protection guidance.
- Finding an online educational resource.
- Practising completion of a demonstration form.
- Using AI to prepare a fictional activity checklist.

Participants should be encouraged to avoid unnecessary disclosure of personal information and to verify important claims through reliable sources.

3.6.20. Completion of Module 3

Module 3 provides practical knowledge and skills related to electronic services and digital participation.

Participants develop familiarity with public administration platforms, digital financial services, online shopping, healthcare information, social support, and community opportunities.

The module also reinforces cybersecurity, privacy, consumer awareness, and responsible decision-making.

Completion should be evaluated through practical activities and demonstrated competencies, taking account of individual learning needs and the level of support required.

3.6.21. Overall Module Conclusion

Electronic services can provide meaningful opportunities for adults to access information, manage everyday activities, and participate more actively in society.

Co-funded by
the European Union

However, successful use requires more than technical access.

Individuals also need appropriate digital competencies, confidence, reliable information, and awareness of potential risks.

Module 3 addresses these needs through accessible explanations, practical demonstrations, realistic scenarios, and structured assessment.

The module supports the development of independent digital participation while recognising the importance of privacy, accessibility, and individual choice.

Together with Modules 1 and 2, it contributes to the broader educational objectives of the Digital Era project by strengthening practical digital literacy, responsible use of artificial intelligence, and informed access to electronic services.

Co-funded by
the European Union