



Co-funded by the
Erasmus+ Programme
of the European Union

**TRAINING PROGRAM FOR
ENHANCING THE USE OF THE MOBILE MONEY BY
ELDERLY
*TRAINER`S GUIDE***



ERASMUS+ MOBILE MONEY

***Training Course for Enhancing the Use of
Mobile Money by the Elderly***



Co-funded by the
Erasmus+ Programme
of the European Union

Contents

METHODOLOGICAL GUIDE	3
COURSE INTRODUCTION	3
COURSE GENERAL FACTS, PREMISES, ORGANISATION AND RESOURCES.....	3
PARTICIPANTS, PROFILES AND NUMBER OF ATTENDANTS.....	4
TRAINING OBJECTIVES.....	5
COMPETENCES TO ACQUIRE AND IMPROVE	6
TRAINING CONTENTS AND MODULES	7
TRAINING METHODOLOGY.....	9
MODULE 1: BASIC DIGITAL LITERACY SKILLS.....	10
MODULE 2: SECURITY & PREVENTION.....	29
MODULE 3: MANAGING A BANK ACCOUNT ONLINE	39
MODULE 4: RECEIVING AND SENDING MONEY	48
MODULE 5: USING A CREDIT CARD TO PURCHASE ONLINE GOODS AND SERVICES	58
MODULE 6: PROCESSING ONLINE PAYMENTS FOR TAXES AND BILLS	70
FINAL THOUGHTS.....	78
BIBLIOGRAPHY	79



Co-funded by the
Erasmus+ Programme
of the European Union

METHODOLOGICAL GUIDE

COURSE INTRODUCTION

This document is drafted in the framework of the **WP3 Development of the Training Package**, of the Erasmus+ project **TRAINING PROGRAM FOR ENHANCING THE USE OF MOBILE MONEY BY ELDERLY** (Ref. 2023-1-RO01-KA220-ADU-000157797). This document will serve as a guide for the development of the training sessions for supporting the adoption of Mobile Money by Elder Persons for managing money and transactions in daily-live situations brought by the digital society. In this document, the contents and the methodology for the final users are presented based on the previous co-creation and co-validation sessions carried out during the project. The Trainer`s Guide includes complete guidelines and training resources for the trainers for supporting the implementation of the training methodology, with step-by step instructions on how to use the training materials for trainees and the Mobile Money Training Tool. To this end, the main objective of this Guide is to present contents, methodologies and tools needed for creating and improving the critical competences of seniors on enhancing their use of mobile money and digital solutions to manage their finance.

COURSE GENERAL FACTS, PREMISES, ORGANISATION AND RESOURCES

The course is divided in six separate modules and has been designed with the next characteristics:

1. The duration of the course is 4-hour session with a total duration of 24 hours, of which:
 - a. Face to face sessions: 2 hours.
 - b. Online sessions: 2 hours (**ONLY IF THE TRAINER DECIDES THAT THE GROUP CAN WORK ONLINE**)

Depending on the specific needs of each group the six modules can be delivered consecutively as part of a 5-6 days training event or each module can be delivered as separate training sessions on different days. It is up to the organizers and the trainers to assess which format best suits the needs of their target group. Each module follows the same methodological guide which consists in 6 sections:

- Objectives
- Competences
- Training contents
- Duration of the session
- Training materials needed for the session: power-point presentations, word handouts, training mobile app tool, practical approach with, scenarios and simulations.



Co-funded by the
Erasmus+ Programme
of the European Union

➤ Learning assessment

The first module includes an introductory session that covers the presentation of the ERASMUS + Program, overview of the project, the objectives and the schedule of the whole training course, participant introductions, expectations and ground rules.

2. The methodology will be active and participative, it will take place in different sessions, and it will include the following tools and training materials:
 - a. Power-point presentations
 - b. Word handouts
 - c. Training mobile app tool
 - d. Mentors or coaches will support trainees during the course
 - e. Practical approach with scenarios and simulations
3. More specifically the Mobile Money Training Tool will be developed with the next purposes:
 - a. Allocation the different training materials and resources with access to trainees.
 - b. Scenarios for practice in a safe simulated space

PARTICIPANTS, PROFILES AND NUMBER OF ATTENDANTS

The trainees will have the following profiles:

- Elderly people with more than 60 years living autonomously or in care facilities.
- Working sessions organised for intermediate revision of the materials with 5 elder persons per country.
- In each pilot setting, it is expected to reach 15 seniors and 5 trainers accompanying them.
- We advise to create different groups of up to 8 seniors. Groups can be determined according to ICT level.
- The entry level requirement is to have access to a place with internet connection and to a smartphone. In order to be able to use the Mobile Money Training Tool, users will need to possess basic



Co-funded by the
Erasmus+ Programme
of the European Union

digital skills, (navigation, security, privacy). A specific module enabling them to acquire them is available in this course.

TRAINING OBJECTIVES

The **general objective** of the training is to improve the competences of older people and their communities for enhancing active aging and autonomy through the use of mobile money and online tools to manage their finances.

Specific objectives are:

- Ensuring seniors have basic digital skills and financial literacy skills for a clear understanding of mobile money solutions and concepts;
- Familiarising seniors with the user interfaces of the most common mobile money apps guiding the through navigation and the main functionalities;
- Educating seniors on security measures to protect their mobile money accounts;
- Introducing mobile tools and techniques for budgeting and tracking expenses;
- Encouraging seniors to share their knowledge within their communities, fostering a sense of community engagement and support in using mobile money tools;
- Highlighting the role of mobile money in promoting social inclusion, enabling seniors to stay connected with friends and family, and participate in the digital economy.

Facilitating opportunities for seniors to engage in peer learning, sharing experiences and tips for effective use of mobile money tools within the group.

GENERAL TIPS FOR COURSE ORGANISATION

The training developed should be used in a flexible way by trainers, it should be seen as a coherent set of tools and resources that should be adapted to each organization and participants' profile and expectations. (e.g the trainer can decide if he will skip the online training or if he wants to resize the group).

The training methodology needs to be adapted to the national context as well as the group. Hence, flexibility is one of the most critical aspects and should be kept in mind by the trainers. The objective of the slides is not to be fully self-explanatory, but the explanations of the trainers and conduction of training sessions is essential.

Trainers should find out from the beginning of the course the participants' needs, preferences and knowledge, so as they could adapt the content and the length of each topic.



Apart from what is provided in the training manual, the trainer should also have some alternative activities/scenarios on hand, so everyone can participate if they think that a certain activity is too difficult or too easy.

COMPETENCES TO ACQUIRE AND IMPROVE

Basic Digital Skills

Necessary skills to use mobile money solutions safely and with confidence:

- Willingness to use ICT devices and keep them up to date
- Managing an email account: sending, receiving, replying to, organising emails, attaching files and managing contacts
- Online navigation
- Setting privacy parameters.

Furthermore, it is important to be familiar with smartphones:

- Understanding basic terminology
- Navigating mobile interfaces and menus
- Using touchscreen and buttons
- Being able to download and update mobile apps.
- Willingness to explore different features of the mobile app.

Security Awareness skills

- Recognizing and avoiding potential scams and phishing attempts
- Securing your ICT devices and mobile money accounts
- Understanding the importance of securing personal information.
- Responding to a security incident

Financial Literacy skills

- Understanding basic financial concepts related to mobile transactions (ie. account balance, transaction history, transaction limits, transaction fees, transfers, bill payment).
- Monitoring account balances and transaction history
- Budgeting and managing finances through mobile apps.

Navigation skills

- Using mobile money apps to send and receive funds
- Navigating through various features such as bill payments, top-ups etc.
- Understanding transaction confirmation messages and receipts.

Problem solving skills

- Ability to troubleshoot common issues independently.
- Seeking help when encountering more complex problems (ie. Contacting customer support and reporting issues).



Co-funded by the
Erasmus+ Programme
of the European Union

Transversal skills

Being more autonomous in the management of personal finances

Being confident in their own skills to manage finances through ICTs.

Trusting new technologies and mobile finance environment

Feeling safe when using the mobile finance environment

Acquiring social skills to interact with their support group, other seniors and providers

TRAINING CONTENTS AND MODULES

MODULE 1. Basic digital literacy skills

1. Introduction of the session: duration, objectives, content and methodology
2. Basic terminology of smartphones
3. Basic settings
4. Navigating interfaces and menus
5. Navigation and search online
6. Managing an email account
7. Searching and downloading an app
8. Keeping ICT devices up to date
9. Quiz: check your knowledge

MODULE 2. Security & Prevention

1. Introduction of the session: duration, objectives, content and methodology
2. Online safety, personal data, sensitive data, privacy and security
3. Recognizing spam and phishing and what to do about them
4. Knowing your online rights, the example of GDPR
5. Protecting yourself online
6. Quiz: check your knowledge

MODULE 3. Managing a bank account online

1. Introduction of the session: duration, objectives, content, and methodology
2. Differences between bank accounts
3. Advantages and challenges of online banking
4. How to install a mobile banking application
5. Obtaining the identification and access codes



Co-funded by the
Erasmus+ Programme
of the European Union

6. Online transfers
7. Account balance monitoring
8. View messages and alerts
9. Tips and exercises
10. Glossary of banking concepts

MODULE 4. Online solutions for receiving and sending money

1. Introduction of the session: duration, objectives, content, and methodology
2. Introduction to digital money transfer
3. Understanding forms and required data
4. Apps for sending and receiving money
5. Identifying and avoid common scams
6. Accessing and understanding your transaction history
7. Quiz: check your knowledge

MODULE 5. Using a Credit Card to Purchase from Online Goods and Services

1. Introduction of the session: duration, objectives, content, and methodology
2. Structure and navigation of e-shop websites
3. Online shopping accounts: create, manage and pay with a credit card
4. Other common online payment methods
5. Risk prevention for safe online shopping
6. Marketing and merchandising insights
7. Shipping goods and tracking orders
8. How to communicate with customer services
9. Quiz: check your knowledge

MODULE 6. Processing online payments for taxes and bills

1. Introduction of the session: duration, objectives, content, and methodology
2. Becoming familiar with tax payment portals
3. Becoming familiar with utility portals
4. Navigate tax and utility portals
5. Make secure online transactions
6. Quiz: check your knowledge



Co-funded by the
Erasmus+ Programme
of the European Union

TRAINING METHODOLOGY

To achieve the aforementioned objectives, it is proposed to develop a **training methodology** based on the following premises:

- The training contents and materials will be adapted and modulated to the learning capabilities and specific needs of the attendants.
- The training will be based on learning through practice and experience; therefore, the training methodology will be quite active and practical.
- The training sessions will take place both in the classroom and online, therefore training materials and training tools will be developed to be used in both training environments.
- The participation of the trainees will be a must during the training courses; therefore, trainers will promote activities in which trainees will be able to interact and exchange experiences and knowledge between them and with different actors.
- A Mobile Money Training Tool will be developed to facilitate learning, to share knowledge and experiences of trainees, and to support training courses through different scenarios allowing the elderly to experience mobile money solutions in a safe environment to build their trust and confidence.

This guide is designed to help trainers and educators teach basic digital competencies to elderly people, enabling them to confidently and safely use mobile money applications. The content is structured to be clear, practical, and accessible to the specific needs and learning pace of older adults.

MODULE 1: BASIC DIGITAL LITERACY SKILLS

OBJECTIVES:

- To know the different types of digital equipment
- To be able to choose the right type of device for one's needs
- To know how to use a smartphone, a tablet and the internet, including an email and downloading an app;
- To ensure a user-friendly and reasonable use of internet and ICT tools while browsing online.



COMPETENCES:

After completing this module, you will:

- Acquire necessary skills to use mobile money solutions safely and with confidence:
 - ✓ Using ICT devices and keep them up to date
 - ✓ Managing an email account: sending, receiving, replying to, organizing emails, attaching files and managing contacts
 - ✓ Navigating online
 - ✓ Setting privacy parameters
- Becoming familiar with smartphones:
 - ✓ Understanding basic terminology
 - ✓ Navigating mobile interfaces and menus
 - ✓ Using touchscreen and buttons
 - ✓ Being able to download and update mobile apps
 - ✓ Explore different features of the mobile app



TRAINING CONTENT:

- Introduction of the session: duration, objectives, content and methodology
- Basic terminology of smartphones
- Basic settings
- Navigating mobile interfaces and menus, using touchscreen and buttons
- Navigation and search online



Co-funded by the
Erasmus+ Programme
of the European Union

- Managing an email account
- Searching and downloading apps
- Keeping ICT devices up to date
- Quiz: Check your knowledge

TRANSVERSAL COMPETENCIES:

- Social skills
- Trust and Confidence
- Financial Literacy
- Digital Literacy

METHODOLOGY:

- **Active and participative**
- **Face to face training:** Dialogue/ Role play/ Team work
- **Online training:** Selected or own produced videos/ Practical implementation of the tips agreed in the classroom/ Some collaborative work/ Simulation

TRAINING MATERIALS:

Face to face sessions:

- Attendance list
- PowerPoint presentation and necessary equipment
- Stationary: writing tools, paper products, organization supplies, office essentials, art supplies

Online training:

- Online materials (PPT, exercise sheet with step-by step instructions)
- Quiz inserted in the PPT.

TOOLS

Senior-Friendly Phones/Tablets: Devices specifically designed for seniors with larger icons, simplified interfaces, and voice commands.



TRAINING ROADMAP

ACTION 1. Opening

Once the attendees have arrived to the classroom, the trainer will introduce himself and welcome the participants. After that, he will present the Erasmus+ Program and give an overview of the project, objectives and the structure of the whole training activity, and the agenda of the session. Next, the trainer will ask participants to introduce themselves, one at a time, and to name the expectation(s) they have for this training. After all participants have named the expectations, the trainer will review the list and explain which of them are likely to be met during this session and which will not, but they might be met in other ways in the future. The trainer will keep the list of expectations posted throughout the session. Distribute the consent forms and ask participants to fill in and sign them.

The trainer will explain to participants that it is helpful to agree together on the ground rules so that the session is effective. He will ask participants what rules would help the training run smoothly, maximize learning, encourage participation, and make everyone feel welcome and respected. He will write participants' responses on the "Ground Rules" sheet of flipchart, e.g.:

- switch off the mobile phones,
- view and treat each other as equals in the training room,
- ask questions at any time,
- provide feedback that is constructive not critical,
- provide each participant with an opportunity to contribute.

The trainer will post the ground rules on a wall where everyone can see them and keep them posted throughout the session, adapting it if necessary.

The trainer will introduce the Erasmus+ Program.

Tools/Training materials:

- PPT1.1 Erasmus+ Program
- PPT1.2 Overview of the project
- PPT1.3 Overview of the Training

ACTION 2. Survey on previous knowledge- Knowledge evaluation T0

A questionnaire will be handed out to the participants in order to evaluate the level of knowledge the participants have. The same questionnaire will be handed out at the end of the training so as to evaluate the progress.



Co-funded by the
Erasmus+ Programme
of the European Union

Tools: Survey on the level of knowledge

ACTION 3. Developing each topic

The trainer will explain each topic of the session, using different training materials but also using practical exercises and experimentation on computers and smartphones:

Basic terminology

In this section, the beneficiaries would learn the basics of digital equipment. To work in a digital environment a digital device is needed. Each device has its pros and cons. Therefore, the session will focus on which device is useful for which specific activity and their functionality.

Digital Devices refers to electronic devices that process, store, and transmit information in a digital format. These devices are essential tools in today's world, enabling people to perform various tasks such as communication, information access, and financial transactions.

Types of Devices: The most common types of digital equipment include smartphones, tablets, laptops, and desktop computers. Each device serves different purposes, but they all share the ability to connect to the internet, run applications and process data. Each device has its pros and cons.

PERSONAL COMPUTER

Description: A personal computer (PC), desktop or laptop, is an electronic device used for a variety of purposes, such as, browsing the Internet, writing documents, playing video games, etc.

Useful for: Advanced web research, writing long texts, writing emails, shopping online goods, e-banking.

Not useful for: Internet research or writing short texts on the move.

SMARTPHONE

Description: A smartphone is a mobile phone that can do much more than just make phone calls. For example, smartphones can connect to the Internet and can take photos or videos. It can also be thought of as a small computer. The screen on a smartphone is a touch screen.

Useful for: Writing short messages, doing a little internet research, using social media like WhatsApp, Instagram, checking emails, e-banking, shopping online.

Not useful for: Writing long texts or doing extensive internet research.



Co-funded by the
Erasmus+ Programme
of the European Union

TABLET

Description: A tablet is smaller than a computer or laptop but larger than a smartphone. It has a touch screen but unlike a laptop, no keyboard.

Useful for: Doing light search activities, downloading and reading books, playing games, watching videos, checking emails, e-banking, shopping online.

Not useful for: Writing long emails or other texts, extensive searching activities.

Memory & Storage: what is the difference?

Imagine your computer is like a desk you use for work.

Memory (RAM) is like the top of your desk where you temporarily place papers and tools you're working with. When you clean it up, elements disappear. Memory is temporary and works fast, but it doesn't keep things forever.

Storage (Hard Drive or SSD) is like a filing cabinet near your desk. This is where you keep your papers, photos, and important documents when you're not using them. The filing cabinet keeps everything safe until you need it again.

So, memory is for "right now" tasks, and storage is for "long-term" keeping. Both are important, but they do different jobs.

Fingerprint and facial recognition: what is the difference?

Fingerprint Recognition

Imagine your fingerprint is like a unique stamp that only you have.

You place your finger on a special sensor, and the device checks the pattern of lines and ridges on your fingertip.

It's like the device saying, "Ah, yes, this is your unique stamp. You're allowed in!"

Facial Recognition

This works like the device "looking" at your face, much like a friend recognizing you when they see you.

It uses the camera to scan the shape of your face, including features like your nose, eyes, and jawline.

The device then says, "Yes, this is your face! Welcome!"

What are settings?

- Think of the settings button like the control panel for your device, just like the dials on your washing machine or TV remote. It's where you go to adjust how things work to suit your needs.

- **How to Recognize the Settings Button:** Look for a symbol that looks like a gear (⚙️).
- **What can you adjust in settings?**



Co-funded by the
Erasmus+ Programme
of the European Union

- **Brightness:** Adjust the screen brightness
- **Volume:** Turn the sound up or down
- **Wi-Fi:** Connect to the internet
- **Language:** Change the language if you prefer reading things in another language.

Using touchscreen and buttons

Touchscreen and buttons are the primary ways to interact with a tablet or smartphone. Understanding how to use them is key to effectively using these devices, especially for elderly users.



Image by pch.vector on Freepik

What is a Touchscreen?

A touchscreen is the part of the device's screen that responds to your touch. Instead of using a mouse or keyboard, you simply use your fingers to control the device.

Basic Touchscreen Actions:

- **Tap:** Gently press your finger on the screen to select something, like an app or a button. It's like clicking a mouse on a computer.
- **Swipe:** Move your finger across the screen to scroll through a page, move between screens, or navigate through photos. This is like flipping through pages in a book.
- **Pinch to Zoom:** Place two fingers on the screen and move them apart to zoom in or bring them together to zoom out. This is useful for making text or images larger or smaller.
- **Hold (Long Press):** Press and hold your finger on an item for a couple of seconds. This usually brings up more options, like when you want to delete or move an app.

Using Physical Buttons:

- **Power Button:** This is used to turn the device on or off. Press and hold the button to turn it on. To turn it off, press and hold until you see an option on the screen, then tap "Power off."
- **Volume Buttons:** These buttons adjust the sound. Press the top button to increase the volume and the bottom button to lower it.
- **Home Button (if available):** On some devices, there's a button that takes you back to the main screen (Home Screen) from any app or page. If there's no physical button, you can usually swipe up from the bottom of the screen to go to the Home Screen.
- **Back Button:** Many devices have a back button, either as a physical button or on the screen, which takes you back to the previous screen or closes the current app.
- **Camera:** Opens the camera to take pictures or videos.



Co-funded by the
Erasmus+ Programme
of the European Union

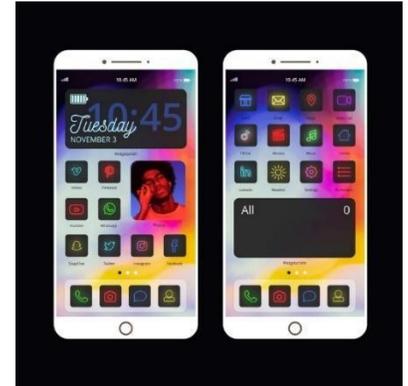
-Gallery/Photos: Lets you view your saved pictures.

Navigating mobile interfaces and menus

Navigating Mobile Interfaces refers to the way you move around and interact with the different screens, apps, and settings on a tablet or smartphone. Understanding this is crucial for using the device effectively.

What is a Mobile Interface?

A mobile interface is the visual part of your device that you see and touch. It includes everything from the home screen (where your apps are) to the menus and settings that control how the device works.



[Image by Freepik](#)

Basic Elements of Mobile Interfaces:

Home Screen: This is the main screen you see when you unlock your device.

It contains app icons (small pictures) that you tap to open different programs, like your phone, messages, or mobile money apps.

App Icons: These are the small images you see on the home screen.

Each icon represents a different app. For example, the phone icon opens the calling app, and the message icon opens the texting app.

<https://guidebooks.google.com/android/usetheappsonyourphone>

Search and download apps:

Android – Google Play Store:

<https://guidebooks.google.com/android/usetheappsonyourphone/downloadapps>

iOS - Apple's App Store

Status Bar: The bar at the top of your screen shows important information like battery life, Wi-Fi connection, and the time.

Navigating Menus:

Home Button: Symbol:  or a square/line at the bottom of the screen.

- **What it does:** Takes you back to the main screen.

Back Button: Symbol:  or an arrow pointing left.

- **What it does:** Goes back to the previous screen.

Wi-Fi: Symbol:  or curved lines.

- **What it means:** Shows if you're connected to the internet.



Co-funded by the
Erasmus+ Programme
of the European Union

Battery: Symbol:

- **What it means:** Displays how much charge is left. A lightning bolt (⚡) shows it's charging.

Camera: Symbol: or a camera icon.

- **What it does:** Opens the camera to take pictures or videos.

Gallery/Photos: Symbol: or a colorful flower/icon.

- **What it does:** Lets you view your saved pictures.

Internet/Browser: Symbol: or a compass/blue circle.

- **What it does:** Opens a web browser to access the internet.

Email: Symbol:

- **What it does:** Opens your email to read or send messages.

Volume/Sound: Symbol: , , , or

- **What it means:** Adjust or mute sound levels.

Gestures:

- **Swipe Up:** Go to the home screen.
- **Swipe Down:** See notifications or quick settings.
- **Pinch to Zoom:** Use two fingers to zoom in or out on pictures or text.



[Image by Freepik](#)

Basic file management

File Management refers to the process of organizing, storing, and accessing different types of files on your tablet or smartphone, such as photos, documents, and apps.

What is a File?

A **file** is any item that you save on your device, such as a photo, video, document, or downloaded app. Just like in a filing cabinet, these files are stored in different folders on your device to keep them organized.

Basic File Management Tasks (This topic is not covered in the PPT or handouts for seniors. However, we believe it is valuable for you as a trainer and can help you address any questions seniors may have on the subject.):

- Finding Files:

Photos and videos are typically stored in the Gallery or Photos app. To find a picture, just open the app, and you'll see all your images.

- Opening Files:



Co-funded by the
Erasmus+ Programme
of the European Union

Tap on the file you want to open. For example, to view a photo, you tap on it in the Gallery app. To read a document, find it in the File Manager app and tap to open it.

- **Moving Files:**

To organize your files, you can move them to different folders. For example, in the File Manager app, you can press and hold on a file until options appear, then select "Move" and choose where you want to place it.

- **Deleting Files:**

If you no longer need a file, you can delete it to free up space. In most apps, this is done by pressing and holding the file, then tapping the trash bin icon or the "Delete" option.

- **Renaming Files:**

To make it easier to find specific files, you can rename them. In the File Manager, press and hold the file, then select "Rename" and type in a new name.

Connecting to the internet, using a browser and Wi-fi

Connecting to the Internet allows your tablet or smartphone to access online services, browse websites, and use apps that require internet connectivity.



[image By Freepik](#)

What is Wi-Fi?

Wi-Fi is a wireless technology that lets your device connect to the internet without needing cables. Wi-Fi is often available at home, in cafes, libraries, or other public places. Your device connects to Wi-Fi through a wireless router, which is a device that broadcasts the internet signal.

How to Connect to Wi-Fi:

1. **Open Settings:** On your device, find and tap the "Settings" app. The icon usually looks like a gear.
2. **Find Wi-Fi Settings:** In the Settings menu, look for an option called "Wi-Fi" and tap it. This will show you a list of available Wi-Fi networks.
3. **Select Your Network:** Tap the name of your Wi-Fi network. If you're at home, this is usually the name of your home network, which your internet provider set up.
4. **Enter Password:** If your Wi-Fi network is secured, a box will appear asking for a password. Type in the Wi-Fi password and tap "Connect." Your device will remember this network, so you won't have to enter the password every time.

Bookmarking: If you find a website you want to return to easily, you can "bookmark" it. Look for a star or a menu option that says "Add to Bookmarks" or "Save." This keeps the site saved in your browser for quick access later.



Co-funded by the
Erasmus+ Programme
of the European Union

Navigation and search online

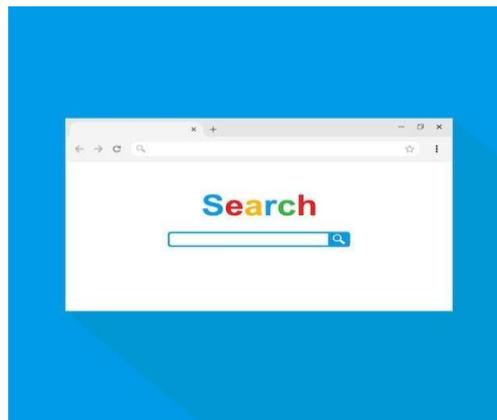
What is a Browser?

A browser is an app that allows you to search for and view information on the internet, like Google Chrome, Safari, or Firefox. It's like a gateway to the web, where you can find websites, read articles, and watch videos.

Using a Browser:

1. Search the Web: You can search for information on the World Wide Web, using any of the devices mentioned above, such as a smartphone, tablet or PC. Once you have decided which device you want to use, there are a number of different steps you should take when searching.

2. Open the Browser App: Look for the browser app on your home screen and tap to open it. The most popular web browsers include: Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari, Opera. At the top of the browser, there's a bar where you can type. This is the address or search bar. Tap on it and type what you want to search for, like "weather today," then press "Enter" or tap the magnifying glass icon. Some of the most popular search engines are: **Google.com**-you can differentiate your search between information, photos or use it to navigate; **Bing.com** -The structure and functionality is usually like Google, but the search results may be different, **Yahoo.com**-very similar to Bing.



[Image by Freepik](#)

3. Navigate Websites: All the information on the Web is available on websites. So, the next step is to connect to the appropriate website that contains the information you are looking for. To connect to a website, you need to know its domain name, e.g, elderlymobilemoney.eu or to use a search engine to find it. And the next questions are: "Which website (s) should I visit to find the information I want? and "How can I find the domain name of this/these website (s)? Once you search, you'll see a list of websites.



Co-funded by the
Erasmus+ Programme
of the European Union

Steps:

- a. The user logs on via browser to search engine
- b. Enter keywords
- c. The search engine returns a list of websites related to the keywords
- d. The user chooses to visit one or more of the websites

Use the "Back" button to return to the previous page, and the "Home" button to return to your starting page.

Web browsers

To search for information on the Web, you need to open a web browser (*step 1*). A web browser is usually already available on your device.

Some of the most popular web browsers include

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Apple Safari
- Opera



[Images by Freepik](#)

Finding the right websites

All the information on the Web is available on websites. So, the next step is to connect to the appropriate website that contains the information you are looking for.

To connect to a website, you need to know its domain name, e.g.,



Co-funded by the
Erasmus+ Programme
of the European Union

elderlymobilemoney.eu

Domain names

To begin with, we have somehow been informed about a domain name by:

- reading it somewhere,
- being told by someone,
- finding it on another website with related content, or
- using a search engine to find the domain name of the website.

Tips:

- If you already know the domain name, you may type it directly into your browser and connect to the website;
- Otherwise, use a **search engine** to find it.

Search engine

A **search engine** is a service for finding websites. It collects websites available on the Web and associates them with various tags, which are keywords related to the main category of information of the website.



Co-funded by the
Erasmus+ Programme
of the European Union

Steps:

1. Enter the URL of the search engine
2. Enters the keywords
3. The search engine returns a list of websites related to the keywords
4. The user chooses to visit one or more of the websites



[Image by Freepik](#)

Using and updating ICT tools

ICT Tools (Information and Communication Technology tools) on a tablet or smartphone include the apps, software, and features that allow you to communicate, access information, and manage tasks. Keeping these tools updated ensures your device runs smoothly, stays secure, and has the latest features.

What Are ICT Tools?

ICT Tools refer to the applications (apps) and features on your device that help you communicate, gather information, and manage tasks. Examples include messaging apps like WhatsApp, email apps, video calling apps like Skype, web browsers, and productivity tools like calendars or notes.

Using ICT Tools:

- 1. Opening an App:** To use an ICT tool, start by finding its icon on your home screen and tapping it. For example, to send an email, tap the email app icon.
- 2. Navigating the App:** Once inside the app, you can use its features by tapping on different buttons or menus. For instance, in a messaging app, tap the "New Message" button to start a conversation.
- 3. Switching Between Apps:** You can switch between different ICT tools by pressing the "Home" button to go back to the home screen and then opening another app. Some devices also allow you to see all open apps by swiping up from the bottom of the screen or tapping a special button.

Updating ICT Tools:

Keeping your apps and software up to date is important for security and performance. Updates often fix bugs, add new features, and protect your device from security risks.

Check for Updates:

- ◆ Open the "App Store" (for iPhone/iPad) or "Google Play Store" (for Android devices).
- ◆ Tap on your profile icon or menu, usually found in the top right corner.



Co-funded by the
Erasmus+ Programme
of the European Union

- ◆ Look for an option that says "Updates" or "Manage Apps & Device."

Update Apps:

- ◆ In the Updates section, you'll see a list of apps that have available updates.
- ◆ You can choose to update individual apps by tapping "Update" next to each app, or update all apps at once by tapping "Update All."

System Updates:

- ◆ System updates are updates to the entire operating system of your device, not just individual apps. These updates are important for keeping your device secure and running well.
- ◆ To check for system updates, go to "Settings," scroll down to "System" or "Software Update," and tap to check if an update is available. Follow the on-screen instructions to download and install the update.

Tips for protecting your data and devices

Software updates are supplied to apply fixes to known application, browser, and operating system security vulnerabilities. They also deploy new or enhanced features, remove outdated features, and improve software stability.

1. Use the **latest versions** of an operating system, install **anti-virus** and firewall software and **check for updates** regularly.
2. Avoid downloading free software from unknown or untrusted websites. Only download software from known and trusted companies, as soon as possible.



[Image by storyset on Freepik](#)

Searching for online information

Searching for online information involves using the internet to find answers, explore topics, and access services like news, weather, or health resources. Your tablet or smartphone makes this process easy and accessible.



Co-funded by the
Erasmus+ Programme
of the European Union

What is Online Search?

Online search is the process of using a search engine, like Google or Bing, to find information on the internet. A search engine is a special website that helps you locate other websites, articles, videos, and more based on the words you type in.

How to Search for Information Online:

1. **Open a Web Browser:** Start by finding and tapping the web browser app on your device, like Google Chrome, Safari, or Firefox. The browser is your gateway to the internet.
2. **Access the Search Bar:** At the top of the browser, you'll see a search bar or address bar. This is where you type in the words or questions you want to search for.
3. **Type Your Search Query:** Tap on the search bar to bring up the keyboard. Type in what you're looking for, like "today's weather," "easy recipes," or "nearest pharmacy." After typing, press the **"Enter"** key or tap the magnifying glass icon to start the search.
4. **Review the Search Results:** The browser will show you a list of websites and information related to your search. Each result is usually a link that you can tap to visit the site and read more.



[Image by Pinterest](#)

5. **Visit a website:** Tap on a link to go to a website. You can scroll through the page, read the information, and explore other parts of the site by tapping on different links or menu items.
6. **Using Voice Search (Optional):** Some devices allow you to search using your voice. Tap the microphone icon in the search bar, then speak your question or keywords. The search engine will then display results based on what you said.



Co-funded by the
Erasmus+ Programme
of the European Union

Tips for Effective Searching:

- ◆ Be Specific: Try to use clear and specific words to get better results. For example, instead of searching "food," try "easy chicken recipes."
- ◆ Check Sources: Make sure the websites you visit are trustworthy, especially for important topics like health or finance.
- ◆ Use Bookmarks: If you find a website you like, you can bookmark it by tapping the star icon or selecting "Add to Bookmarks" so you can easily find it later.

Managing an email account

Managing an email account on your device involves checking, sending, organizing, and maintaining your emails. It's an important way to stay in touch with family, friends, and services.

Objectives:

- To know how to get an email account
- To manage an email account: sending, receiving, replying to, organizing
- emails, attaching files and managing contacts.



What is an Email Account?

An email account is a service that lets you send and receive digital messages (emails) over the internet. You access your emails using an app on your device, like the Mail app, Gmail, or another email app. The exchange (sending and receiving) of email is still popular for **formal written** communication with your professional peers. Emails can be archived, electronically or printed, and provide proof of communication. You can also always read them to remember details.

We can say that the email communication could be:

- **Informal**, like the way we communicate with people we are very close to, such as our family members and friends;
- **Formal**, which includes a formal way of communicating with organizations and people we do not know or have a professional relationship with;
- **Semi-formal**, which is between informal and formal, e.g., you might consider using this type for sending email to your doctor.



Co-funded by the
Erasmus+ Programme
of the European Union

How to Manage Your Email Account:

1. Setting Up Your Email Account:

If it's your first-time using email on the device, you need to set up the account. Open the email app (like Gmail or Mail) and follow the on-screen instructions to enter your email address and password. Once set up, your emails will automatically come to your device.

2. Checking Emails:

- Open the email app by tapping its icon on your home screen. When the app opens, you'll see a list of your recent emails in your inbox. Tap on any email to open and read it.

3. Sending an Email:

- To send a new email, look for a button labelled "Compose," "New," or a plus sign (+). Tap it, and a blank email form will appear.

- In the "To" field, type the recipient's email address.

- In the "Subject" field, type a short description of your email.

- In the main body, type your message. When you're ready, tap "Send."

4. Replying to Emails:

- When you open an email, you'll see options to "Reply" or "Reply All" at the bottom. Tap "Reply" to send a response to the person who sent you the email. Type your message, then tap "Send."

5. Deleting Emails:

- To keep your inbox organized, you may want to delete emails you no longer need. In your inbox, press and hold the email you want to delete, then tap the trash bin icon or "Delete" option.

6. Organizing Emails:

- To help you find your way around your inbox, you can **organise it by creating subsections** and sorting your emails within them. Depending on your email service, this may be called 'labels' or 'folders'.

- When you only want to search for emails that you have labelled in a specific sub-section, click on the Menu button in your mailbox, then choose the section you want to appear. To return to the general view, click on the Menu button again.

Please note: the use of this organization system varies depending on the email service. If you are in any doubt, check the service user guide first.



Co-funded by the
Erasmus+ Programme
of the European Union



Image by Freepik



Image of storyset on Freepik

Search a specific email

To find an email easily, you can also filter your mailbox:

- Click on the search bar at the very top of the home page.
- Several drop-down menus will appear below (From, To, Date etc).
- Enter your search criteria.
- The corresponding emails will then be displayed directly.
- If not, click on Search to display the emails.

7. Managing Spam and Junk Mail:

● Some emails you receive may be spam (unwanted or suspicious messages). Most email apps automatically move these to a "Spam" or "Junk" folder. If you find spam in your inbox, you can move it to the spam folder by selecting the email and tapping "Move to Spam" or "Mark as Spam."

Tips for protecting your data and devices

Software updates are supplied to apply fixes to known application, browser, and operating system security vulnerabilities. They also deploy new or enhanced features, remove outdated features, and improve software stability.

1. Use the latest versions of an operating system, install anti-virus and firewall software and check for updates regularly.
2. Avoid downloading free software from unknown or untrusted websites. Only download software from known and trusted companies, as soon as possible.



Co-funded by the
Erasmus+ Programme
of the European Union

Search and download apps

To download an application, always use the online shop accessible from your smartphone, to make sure you only download safe applications:

Android – Google Play Store



Iphone – Apple's App Store



On these shops, it works in the same way as an internet search. Search directly for an application if you know its name, or for a theme that interests you, and explore the different choices on offer.

Then click on the 'Install' or 'Get' button (depending on the shop and app) to start the download. Once the download is complete, you can access it directly on your smartphone.

Practical exercise

Create a new label to organize your emails

Try creating a label (or equivalent) to sort your emails:

1. In your mailbox menu, look for the 'Labels' section (or equivalent), and click on 'Create new'.
2. Personalize it, by giving it a name and a color for example.
3. Click on 'Done'.
4. Next, open an email that you want to add under this label.
5. Click on the mail options button, and click on 'Change label'.
6. Choose the right label for this email, and click 'Apply'.
7. View the results on the first page: Do you see the label symbol appearing next to your email?

Try a second method: drag and drop a second email into the label you've created, visible on the left-hand side of your email (depending on your type of email, only one of these methods may be available).

Action 4. Debriefing and Closure

The trainer summarizes the content of the session and clarifies possible doubts and questions. The trainer explains the activities to be done in the next online training session.

MODULE 2: SECURITY & PREVENTION

This module focuses on enhancing the security and prevention skills necessary for using mobile money solutions safely. The primary objectives are to understand basic security principles, secure ICT or mobile devices, secure mobile money accounts, recognize and report scams and phishing, and verify transaction details while keeping receipts.

OBJECTIVES

- Understand basic security principles.
- Secure ICT or mobile devices.
- Secure mobile money accounts.
- Recognize and report scams and phishing.
- Verify transaction details and keep receipts.



COMPETENCES

Participants will acquire the necessary skills to use mobile money solutions safely and with confidence.



They will learn to:

- Use ICT devices and keep them up to date
- Manage an email account.
- Navigate online securely.
- Manage basic files
- Set privacy parameters.
- Navigate mobile interfaces & menus
- Use touchscreen and buttons
- Explore mobile features

TRAINING CONTENT

1. Introduction to Online Safety, Personal Data, and Privacy

- Definition and examples of personal data, including sensitive personal data.
- Privacy vs. Security.
- GDPR compliance and its importance in protecting personal data.



[Image by Freepik](#)



Co-funded by the
Erasmus+ Programme
of the European Union

2. Securing ICT or Mobile Devices

- Importance of strong passwords.
- Best practices for safeguarding personal information online.
- Using biometric authentication (fingerprint, facial recognition) and PINs.
- Regularly updating operating systems and antivirus software.

3. Securing Mobile Money Accounts

- Best practices for keeping mobile money accounts secure.
- Importance of two-factor authentication.
- Verifying transaction details and keeping online receipts.

4. Recognizing and Reporting Scams

- Understanding phishing and spam.
- Identifying suspicious emails.
- Reporting security incidents.

TRANSVERSAL COMPETENCES

- **Social Skills:** Enhancing communication and interaction within the group.
- **Trust and Confidence:** Building trust in using mobile money solutions.
- **Financial Literacy:** Understanding financial concepts related to mobile transactions.
- **Digital Literacy:** Improving overall digital skills and confidence.

METHODOLOGY

The training methodology for this module includes both face-to-face and online training. Face-to-face training involves dialogue, role-playing, and teamwork, while online training includes videos, practical exercises, collaborative work, and simulations. This blended approach ensures that participants can engage with the material in various ways, enhancing their learning experience.

TRAINING MATERIALS

- PowerPoint presentations.
- Word handouts for practical exercises
- Quiz in the PPT.



Image by Freepik

TOOLS

- **Senior-Friendly Phones/Tablets:** Devices specifically designed for seniors with larger icons, simplified interfaces, and voice commands.
- **Interactive Quiz Platforms:** Tools like Kahoot! for engaging quizzes.
- **Role-Playing Scenarios:** Predefined scenarios for practical exercises.



Co-funded by the
Erasmus+ Programme
of the European Union

- **Secure Transaction Simulation:** Mobile Money app for practicing secure transactions.

TRAINING ROADMAP

ACTION 1. Opening

The trainer welcomes back all the participants and invites them to get comfortable for a new training session. He/she summarizes the content of the previous session in order to help participants remember the key points and after this, the trainer lets the participants know what to expect from this session: duration, main topics, objectives, necessary tools.

ACTION 2. Developing each topic

The training content is divided into several key sections and the trainer presents them as follows:

INTRODUCTION TO ONLINE SAFETY, PERSONAL DATA, AND PRIVACY

The first section, "Introduction to Online Safety, Personal Data, and Privacy," covers the definition and examples of personal data, including sensitive personal data such as racial or ethnic origin, political opinions, religious beliefs, genetic data, biometric data, health data, and data concerning a person's sex life or sexual orientation. It also explains the difference between privacy and security and the importance of GDPR compliance in protecting personal data.

Being online exposes Internet users to **online security** threats. Once a user sends data over the Internet (video or voice call packets, chat, email or credit card numbers, websites) they have no control over who can access the data. Data passes through many servers, routers, and devices where any hacker, service provider or government agent can access and read it.

Personal data is any information relating to a **living, identified or identifiable individual**.

Examples of personal data are as follows:

- Name and surname;
- Home address;
- Email address such as *name.surname@company.com*;
- Location data, such as the location data function on a mobile phone);
- Identification card number;
- Internet Protocol (IP) address;



Co-funded by the
Erasmus+ Programme
of the European Union

- A cookie ID;
- Your phone's advertising ID;
- Data held by a hospital or doctor, which may be a symbol that uniquely identifies a person.

Here is an overview of the first section:

- **Definition and Examples of Personal Data:** Personal data includes any information relating to an identified or identifiable individual, such as name, address, email, IP address, and more.
- **Sensitive Personal Data:** Data revealing racial or ethnic origin, political opinions, religious beliefs, genetic data, biometric data, health data, and data concerning a person's sex life or sexual orientation.
- **Privacy vs. Security:** Privacy is about controlling personal data and how it is used by third parties, while security is about protecting data from unauthorized access.
- **GDPR Compliance:** Understanding the General Data Protection Regulation and its importance in protecting personal data.

What is Security?

Security is about **how to secure, protect your personal data** from **unauthorized access**, whether on your device, on the remote web server or during communication over the Internet.

We use **security controls** at a technical level to limit who can access the information. These controls are in place:

- On our devices (PC, tablet, mobile phone), i.e., applying operating system and software updates, using strong passwords;
- On the remote web server, i.e., use strong passwords;
- When submitting information over the Internet, i.e., use the secure **https** protocol.



[Image by vectorjuice on Freepik](#)

Sensitive financial data

- Account and password for an e-banking system
- The CCV, date of expiry of a credit or debit card
- The PIN code of your mobile phone

→ Examples and exercise



Image by redgreystock on Freepik

Security and Privacy

- Security is about **protecting data**, while privacy is about **protecting the identity of users**.
For example, hospital and clinic staff use secure systems to communicate with patients about their health, rather than sending information via personal email accounts. This type of communication is an example of security.
- On the other hand, privacy policy and provision might limit access to patient's health records to **certain hospital staff members**, such as doctors, nurses, and medical assistants.

- **It is possible to have security without privacy.**
Indeed, **for example**, personal data can be securely transmitted and stored on a website securely, but the website can still sell it.
- **It is not possible to have privacy without security.**
Indeed, **for example**, a hacker could gain unauthorized access to your device, web server or transmitted data and steal your personal data

SECURING ICT OR MOBILE DEVICES

"Securing ICT or Mobile Devices," emphasizes the importance of creating and using strong, unique passwords for different accounts. Participants will learn best practices for safeguarding personal information online, using biometric authentication (fingerprint, facial recognition) and PINs to secure devices, and regularly updating operating systems and antivirus software to protect against vulnerabilities.



Co-funded by the
Erasmus+ Programme
of the European Union

The **General Data Protection Regulation** is a European Union law that was implemented on May 25, 2018, that requires organizations to protect personal data and uphold the privacy rights of everyone in EU territory.

When discussing this topic, focus on:

- **Strong Passwords:** Importance of creating and using strong, unique passwords for different accounts.
- **Protecting Personal Information:** Best practices for safeguarding personal information online.
- **Biometry and PINs:** Using biometric authentication (fingerprint, facial recognition) and PINs to secure devices.
- **Keeping Systems Updated:** Regularly updating operating systems and antivirus software to protect against vulnerabilities.

SECURING MOBILE MONEY ACCOUNTS

In the third section, "Securing Mobile Money Accounts," participants will learn practices for keeping mobile money accounts secure, such as using strong passwords and enabling two-factor authentication. The importance of using two-factor authentication for an added layer of security will be highlighted, along with the need to verify transaction details before confirming and keeping online receipts for records.

Security is about **how to secure & protect your personal data** from **unauthorized access**, whether on your device, on the remote web server or during communication over the Internet.

Here are the highlights of this section:

Securing Mobile Money Accounts

- **Account Security:** Tips for keeping mobile money accounts secure, such as using strong passwords and enabling two-factor authentication.
- **Double Authentication:** Importance of using two-factor authentication for an added layer of security.

Spam and phishing

You may have received annoying emails from an **unknown sender**, usually of a commercial nature. In addition, **emails can be dangerous because** they may contain links that lead to phishing websites or websites that host malware or contain malware as an attachment.

So, **do not open any attached files or click on any links**. And never, give out your personal data, e-banking account details (any username, password), or details of your credit/debit card, such as the expiry date and the 3-digits CCV.

This, is called **phishing**: criminals send official-looking emails to trick you into revealing details that can be used for identity theft.

How do I identify spam?

An email is suspicious if it contains one or more of the following

- Grammar and spelling errors
- Mails in a foreign language
- The sender's name is missing
- Urgent need for action - especially in combination

with a threat

- Prompt to enter personal data (e.g., PIN or TAN)
- Request to open a file
- Never received any emails from the bank or a

customer



Image by Freepik

RECOGNIZING AND REPORTING SCAMS

This section focuses on understanding phishing and spam, identifying suspicious emails, and reporting security incidents. Participants will learn to recognize common signs of phishing emails, such as grammar errors, urgent requests for action, and prompts to enter personal data.

- Avoid opening attachments unless they have been scanned by an anti-virus programme.
- Remember to log out, especially if you are using a shared public computer.
- Delete all emails from unknown people.
- Never reply to spam!
- Do not click on links in spam emails.

These are the main topics of this section:

- **Understanding Phishing and Spam:** Identifying phishing attempts and spam emails that aim to steal personal information.
- **Identifying Suspicious Emails:** Signs of suspicious emails, such as grammar errors, urgent requests for action, and prompts to enter personal data.
- **Reporting Security Incidents:** Steps to report phishing threats and spam to relevant authorities or service providers.



Co-funded by the
Erasmus+ Programme
of the European Union

What are your online rights and how you can protect yourself in advance?

We are digital citizens

Digital citizens can enjoy rights of privacy, security, access and inclusion, freedom of expression and more.

However, with those rights come certain responsibilities, such as ethics and empathy and other responsibilities to ensure a safe and responsible digital environment for all.



[Image by pch.vector on Freepik](#)

What is GDPR and who needs to comply with it?

Even if an organization has no connection to the EU itself, but processes personal data of people in the EU (for example, through tracking on its website), it still needs to comply with the GDPR.

The GDPR is also not limited to for-profit companies.

- GDPR protects your rights as a user
- It is good that you know and practice your consents and cookies.
- The effective management of vulnerable customers is an absolute must, not only as a regulatory expectation but also because it is socially responsible and good business practice.

OTHER Some examples for you to be safe

● Avoid paying anyone through wire transfer, Western Union, money order, or gift cards. Scammers often ask for these types of payments since they do not leave a traceable paper trail.

● Never share your passwords with anyone online. Only with the trusted person like a daily member.

● Be skeptical of anything urgent. Scammers often want you to act before you have time to think critically about the situation. Remember to pause and perhaps walk away from the computer instead of panicking if you think something is suspicious and you're not sure how to proceed.

- Immediately click the X or No to close any websites or pop-ups about viruses or sweepstakes.
- Call a loved one or search online for advice (e.g., typing "We need support urgently...")
- Check in Google to see if other people have reported such scams.
- Ensure that websites have <https://> listed in front of them. The "s" indicates that the site is secure. The name should also have a little lock next to it.
- Be wary of anything that seems too good to be true.
- Consider turning on multi-factor authentication. This requires you to either enter a code (sent via text or email) or use an app to log in to some of your accounts, including social media or banking portals. This can prevent hackers from signing in.
- More precautions can be taken to avoid scams.



Co-funded by the
Erasmus+ Programme
of the European Union

- No one needs to be fearful of continuing to use the internet, so long as they are equipped with the knowledge of how to use it safely.
- Find a safe space in your community or social circle where you can feel comfortable discussing these issues without fear of being judged.
- If a scam has already taken place, here are some actionable steps that you can take:
- Call your bank. They can freeze your account so that no one can access your funds and also issue you a new debit card. If money has already been stolen, you can see if the bank can void those transactions and return your funds.
- Consider filing a police report.

OTHER ENGAGING ACTIVITIES YOU CAN TRY

To make the training more interactive and engaging, several activities are included:

1. **Password Strength Challenge:** This activity teaches participants the importance of strong passwords. Participants are divided into small groups and provided with a list of weak passwords. They are then asked to transform these into strong passwords using guidelines, and each group presents their strong passwords and explains their choices.
2. **Phishing Email Identification:** This activity helps participants recognize phishing emails. Trainers show examples of real and fake emails on a screen and ask participants to identify which emails are phishing attempts and explain why. This activity includes a discussion on common signs of phishing emails.
3. **Secure Your Device Relay:** In this activity, participants move from station to station, completing different security tasks such as setting up a PIN, enabling two-factor authentication, and updating antivirus software. This activity is timed, and the fastest team is rewarded with a small prize.
4. **Role-Playing Scenarios:** Participants practice responding to security incidents through role-playing. Trainers create scenarios where participants must respond to a security incident, such as receiving a suspicious email or noticing unusual account activity. Participants discuss their actions and decisions, and the group debriefs to highlight best practices and lessons learned.
5. **Interactive Quiz:** Using a platform like Kahoot! (This quiz reinforces knowledge of security principles. Participants answer questions in real-time using their devices, and the correct answers are discussed with additional explanations provided as needed).
6. **Secure Transaction Simulation:** This activity involves using the Mobile Money app to simulate making a secure transaction. Participants follow step-by-step instructions to complete a transaction, ensuring they verify details and keep receipts. This activity emphasizes the importance of each step and how to recognize secure transaction practices.
7. **Data Privacy Discussion:** This activity facilitates a group discussion on data privacy using real-world examples of data breaches and their consequences. Participants share their thoughts on how



Co-funded by the
Erasmus+ Programme
of the European Union

they protect their personal data, and trainers provide tips and best practices for maintaining data privacy.

Action 3. Debriefing and Closure

The trainer summarizes the content of the session and clarifies possible doubts and questions. The trainer explains the activities to be done in the next online training session.

MODULE 3: MANAGING A BANK ACCOUNT ONLINE

This module focuses on teaching participants how to manage a bank account online. The primary objectives are to set up and manage an online bank account, use common functions of an online bank account, and understand the differences between traditional and online banking.

OBJECTIVES

- Set up and manage an online bank account.
- Use common functions of an online bank account.
- Understand the differences between traditional and online banking.



COMPETENCES

Participants will acquire the necessary skills to manage their finances through online banking. They will learn to:

- Create and manage an online bank account.
- Identify and access online banking services.
- Make transfers and pay bills online.
- Monitor account balance and transactions.
- View messages and alerts.



TRAINING CONTENT

1. Types of Bank Accounts

- Differences between traditional and online bank accounts.
- Savings vs. current accounts.

2. Advantages and Challenges of Online Banking

- Convenience and time-saving benefits.
- Security concerns and solutions.

3. Setting Up an Online Bank Account

- Steps to create an account.
- Obtaining identification and access codes.
- Verifying identity and creating a username and password.

4. Managing an Online Bank Account

- Accessing services offered by the account.



Co-funded by the
Erasmus+ Programme
of the European Union

- Making transfers and paying bills.
- Consulting account balance and transactions.
- Understanding messages and alerts

5. Practical Exercises

- Question and answer matching.
- Converting a regular bank account into an online bank account.
- Using the Mobile Money app to practice online banking functions.
- Making a bank transfer.
- Monitoring account balance and viewing alerts.

TRANSVERSAL COMPETENCES

- **Social Skills:** Enhancing communication and interaction within the group.
- **Trust and Confidence:** Building trust in using online banking solutions.
- **Financial Literacy:** Understanding financial concepts related to online banking.
- **Digital Literacy:** Improving overall digital skills and confidence.

METHODOLOGY

The training methodology for this module includes both face-to-face and online training. Face-to-face training involves dialogue, role-playing, and teamwork, while online training includes videos, practical exercises, collaborative work, and simulations. This blended approach ensures that participants can engage with the material in various ways, enhancing their learning experience.

TRAINING MATERIALS

- PowerPoint presentations.
- Word handouts with practical exercises
- Training mobile app tool with simulation
- Quiz inserted in the PowerPoint

TOOLS

- **Senior-Friendly Phones/Tablets:** Devices specifically designed for seniors with larger icons, simplified interfaces, and voice commands.
- **Interactive Quiz Platforms:** Tools like Kahoot! for engaging quizzes.
- **Role-Playing Scenarios:** Predefined scenarios for practical exercises.
- **Secure Transaction Simulation:** Mobile Money app for practicing secure transactions.



Co-funded by the
Erasmus+ Programme
of the European Union

TRAINING ROADMAP

ACTION 1. Opening

The trainer welcomes back all the participants and invites them to get comfortable for a new training session. He/she summarizes the content of the previous session to help participants remember the key points and after this, the trainer lets the participants know what to expect from this session: duration, main topics, objectives, necessary tools.

ACTION 2. Developing each topic

The training content is divided into several key sections and the trainer presents them as follows:

TYPES OF BANK ACCOUNTS

This section introduces participants to the different types of bank accounts available, focusing on the distinctions between traditional and online bank accounts. Traditional banking typically involves in-person interactions at physical branches, where customers use savings books and cash for transactions. In contrast, online banking allows customers to perform transactions remotely via an app or the bank's website, offering greater convenience and flexibility. Participants will also learn about the differences between savings and current accounts, understanding their specific purposes and features. This foundational knowledge is crucial for making informed decisions about which type of account best suits their needs.

Traditional Banking	Online Banking
Banking operations require going to a branch and communicating in person for any transaction. Thanks to the ATM it is possible to withdraw money in person, but it is still necessary to travel.	Online banking services are usually not very different from traditional banking services, but they have the special feature that they can be performed remotely via an app or the bank's own website.

Here are the main topics of this section:

- **Differences between Traditional and Online Bank Accounts:** Traditional banking relies on in-person interactions and physical branches, while online banking allows transactions to be performed remotely via an app or website.
- **Savings vs. Current Accounts:** Understanding the different purposes and features of savings and current accounts.

ADVANTAGES AND CHALLENGES OF ONLINE BANKING

In this section, participants will explore the various advantages and challenges associated with online banking. The convenience of 24/7 access, the ability to save time by avoiding queues, and the potential for lower fees are significant benefits of online banking. Additionally, online banking provides easy management of accounts with real-time balance tracking. However, participants will also learn about the challenges, such as the lack of personal contact with bank staff, a smaller network of ATMs, and potential security concerns. Understanding these pros and cons will help participants weigh their options and adopt best practices for secure and efficient online banking.

Traditional Banking	Online Banking
<p>Advantages</p> <ul style="list-style-type: none"> • Personal Attention: Direct contact with the bank teller • Ample availability of ATMS • Additional services (security boxes, insurance services) <p>Disadvantages</p> <ul style="list-style-type: none"> ▪ Limited opening hours ▪ Waiting time of each visit 	<p>Advantages</p> <ul style="list-style-type: none"> • Convenience: 24/7 access without travel • Time-saving: no waiting in lines • Less commissions • Easy management: real-time balance tracking <p>Disadvantages</p> <ul style="list-style-type: none"> ▪ No reference person for direct contact ▪ Small network of ATMs

The highlights of this topic are:

- **Advantages:** Convenience, 24/7 access, time-saving, less commission, and easy management with real-time balance tracking.
- **Challenges:** Lack of personal contact, smaller network of ATMs, and security concerns.

Steps to access the online account for the first time

2/2

- Verify your identity by following the bank's instructions, which may include sending a verification code to your phone or email.
- Once your identity has been verified, you will be able to access your online banking account with your username and password.

Remember to keep your login information secure and do not share it with anyone



Image by [IberCaja](#)



Co-funded by the
Erasmus+ Programme
of the European Union

SETTING UP AN ONLINE BANK ACCOUNT

This section provides a step-by-step guide on how to set up an online bank account. Participants will learn the process of visiting the bank's website, registering for an account, and filling in the required personal information. The importance of creating a strong username and password will be emphasized, along with the steps to verify their identity, which may include receiving a verification code via phone or email. Additionally, participants will be guided on how to obtain identification and access codes from their bank, either directly at a branch or through the bank's website. This comprehensive guide ensures that participants can confidently set up their online bank accounts and access the necessary services.

These are the primary topics of this section:

- **Steps to Create an Account:** Visiting the bank's website, registering, filling in personal information, creating a username and password, and verifying identity.
- **Obtaining Identification and Access Codes:** Requesting access data from the bank and logging in with the provided details.

MANAGING AN ONLINE BANK ACCOUNT

In this section, participants will learn how to effectively manage their online bank accounts. They will be introduced to the various services offered by online banking, such as making transfers, paying bills, and consulting account balances and transactions. Detailed instructions will be provided on how to make a bank transfer, including entering recipient details, the amount, and the payment reference. Participants will also learn how to monitor their account balance and view transaction history through the online banking interface. This practical knowledge will enable participants to manage their finances efficiently and securely using online banking tools.

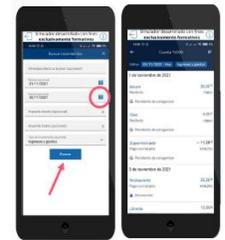


Image by CVR DUTPA, Shutterstock 32

How to make a bank transfer?

<https://youtu.be/7tAHOJAGtn0>

- In the case of a bank transfer, money is transferred from one account to another.
 - Once a transfer has been authorised, it can no longer be cancelled.
 - Have all the information you need at hand. You will find most of the information on the invoice you want to pay (name of the recipient, IBAN, amount and payment reference).
- 

Additional information


- The typical bank transfer screen consists of the following fields:
 - Sender account: the account you want to send the money from
 - Amount: the amount you want to transfer
 - Balance: Balance, you have on your account
 - Recipient: the name you put on the invoice
 - IBAN: 24-digit international bank account identification number
 - BIC: Identifies the destination bank
 - Payment reference: the reason for this payment or the reference on the invoice
 - Date of execution: The date when the transfer should be made

Read below the focus points of this section:

- **Accessing Services:** Identifying and accessing services offered by the online account, such as transfers, bill payments, and balance consultations.
- **Making Transfers and Paying Bills:** Steps to make a bank transfer, including entering recipient details, amount, and payment reference.
- **Consulting Account Balance and Transactions:** Monitoring account balance and viewing transaction history through the online banking interface.

Advantages of making a bank transfer online

- You don't need to carry banknotes from one place to another, so they can't be stolen or lost. In return, the money is protected by the security system of the online bank account.
- A transfer from one account to another at the same bank is free of commission and will be available in the other account immediately.
- There is no need to fill in the transfer order by hand at the bank and you can save the details of the destination account in the app so that you don't have to take these details out for the next transfer.



Co-funded by the
Erasmus+ Programme
of the European Union

Monitoring of account balance

How can I consult the movements of my account online?

There are several ways of accessing the information on your bank transactions:

- You can consult the details of the movements online from the '**Transactions**' menu by clicking on the specific movement you are looking for and the information will be displayed. You can directly download the receipt for that movement.

- If you are looking for the receipt of a supply, consult the '**Direct debits**' menu.

If you are looking for a transfer or a transfer, select **Transfers** > Received/Emitted from the menu and use the search engine.

Messages and alerts

The app sends **alerts** and **messages** via:

- push notifications
- emails, or
- messages within the app itself.
- The most important messages and alerts that can be consulted in the online account include:
 - **Transaction** alerts
 - **Safety** alerts

Common transaction alerts

Transaction alerts:

- **Deposits:** Notification of incoming money
- **Withdrawals or purchases:** Confirmation of card payments or transfers, withdrawals from ATMs.
 - **Account movements:** Notification of transfers, cheque payments, etc.)
 - **Account balance and activity alerts:**
 - Low balance
 - Balance available

Safety alerts:

- **Access not authorized:** Alerts about suspicious access attempts
- **Password change:** Warnings when password or login details are changed
- **Fraud alerts:** Messages alerting to unusual activity
- **Two-factor authentication:** Confirmation of security authentication when logging in or performing a transaction

View messages and alerts



Co-funded by the
Erasmus+ Programme
of the European Union

In addition, messages and alerts can be viewed with the following steps:

1. **Log in to the online banking app**
2. **Access the main menu or the home screen**
 - Messages and alerts can be viewed in the following sections:
 - **Notifications** or **Alerts** (with a little bell or similar icon).
 - **Messages** or **Message centre** (an envelope icon or chat bubble)



Image by [Freepik](#)

3. **View alerts or notifications:**

- Tap the notifications icon to access your alert history.
- Read the details of each alert by clicking on it.
- If the bank has an internal messaging system, go to the Messages or Message Centre section.

ENGAGING ACTIVITIES YOU CAN TRY:

1. **Account Setup Simulation:** Participants simulate setting up an online bank account, including creating a username and password, and verifying identity.
2. **Bank Transfer Relay:** Participants move from station to station, completing steps to make a bank transfer, such as entering recipient details and verifying transaction information.
3. **Role-Playing Scenarios:** Participants practice managing online banking tasks through role-playing scenarios, such as making a transfer or consulting account balance.
4. **Interactive Quiz:** Using a platform like Kahoot! this quiz reinforces knowledge of online banking principles. Participants answer questions in real-time using their devices, and the correct answers are discussed with additional explanations provided as needed.
5. **Secure Transaction Simulation:** This activity involves using the Mobile Money app to simulate making a secure transaction. Participants follow step-by-step instructions to complete a transaction, ensuring they verify details and keep receipts.
6. **Banking Concepts Discussion:** Facilitating a group discussion on basic banking concepts, such as the differences between traditional and online banking, and the advantages and challenges of each.

Frequent terms used in online banking

- **Account Holder:** The owner of the money in the bank account.
- **Direct debit:** To direct debit means to instruct those specific charges and payments be debited from the account (e.g. costs of telephone, electricity, gas).
- **Overdrawn:** 'To be overdrawn' means to have an insufficient balance in the bank account.
- **BIC** (Bank Identifier Code) or **SWIFT** code: identifies the destination bank of a transfer.



Co-funded by the
Erasmus+ Programme
of the European Union

- **PIN:** The 'Personal Identification Number' together with the user number are your access data for your online banking.
- **IBAN** (International Bank Account Number): a 24-digit set of two letters and 22 numbers:
 1. **Country:** The letters identify the country and are linked to two check digits (DC) which serve to validate the entire IBAN
 2. **Entity:** The first four digits are assigned by the Bank of Spain and identify the bank.
 3. **Branch:** The next four digits identify the specific branch where the customer holds the account
 4. **DC:** Again, 2 control digits.
 5. **Account number:** The last 10 digits form the last 10 digits

Action 3. Debriefing and Closure

The trainer summarizes the content of the session and clarifies possible doubts and questions. The trainer explains the activities to be done in the next online training session.

MODULE 4: RECEIVING AND SENDING MONEY

This module focuses on teaching participants how to receive and send money using digital platforms. The primary objectives are to understand the basic digital skills needed for mobile money transfers, identify the necessary information for sending money, and recognize and avoid common scams.

OBJECTIVES

- Understand basic digital skills for mobile money transfers.
- Identify the necessary information for sending money.
- Recognize and avoid common scams.
- Access and understand transaction history.



COMPETENCES

Participants will acquire the necessary skills to perform digital transactions confidently. They will learn to:

Understand and Perform Digital Transactions

- ✓ Identify the necessary information for sending money.
- ✓ Know what IBAN stands for and how to use it.
- ✓ Understand the purpose of a username.
- ✓ Know when and why to use phone numbers.
- ✓ Add clear payment details.

Navigate Security Steps Confidently

- ✓ Understand how PINs protect your account.
- ✓ Use passwords effectively and safely.
- ✓ Recognize SMS codes as an added layer of security.
- ✓ Avoid sharing sensitive details with others.
- ✓ Identify signs of secure connections (e.g., padlock icons).



TRANSVERSAL COMPETENCIES

- **Social Skills:** Enhancing communication and interaction within the group.
- **Trust and Confidence:** Building trust in using digital money transfer solutions.
- **Financial Literacy:** Understanding financial concepts related to digital transactions.
- **Digital Literacy:** Improving overall digital skills and confidence.



Co-funded by the
Erasmus+ Programme
of the European Union

METHODOLOGY

The training methodology for this module includes both face-to-face and online training. Face-to-face training involves dialogue, role-playing, and teamwork, while online training includes videos, practical exercises, collaborative work, and simulations. This blended approach ensures that participants can engage with the material in various ways, enhancing their learning experience.

TRAINING MATERIALS

- PowerPoint presentations.
- Word handouts with practical exercises
- Training mobile app tool.

TOOLS

- **Senior-Friendly Phones/Tablets:** Devices specifically designed for seniors with larger icons, simplified interfaces, and voice commands.
- **Interactive Quiz Platforms:** Tools like Kahoot! for engaging quizzes.
- **Role-Playing Scenarios:** Predefined scenarios for practical exercises.
- **Secure Transaction Simulation:** Mobile Money app for practicing secure transactions.

TRAINING ROADMAP

ACTION 1. Opening

The trainer welcomes back all the participants and invites them to get comfortable for a new training session. He/she summarizes the content of the previous session in order to help participants remember the key points and after this, the trainer lets the participants know what to expect from this session: duration, main topics, objectives, necessary tools.

ACTION 2. Developing each topic

The training content is divided into several key sections and the trainer presents them as follows:



Co-funded by the
Erasmus+ Programme
of the European Union

INTRODUCTION TO DIGITAL MONEY TRANSFERS

This section introduces participants to the concept of digital money transfers, which allow individuals to send or receive money electronically using mobile apps or online platforms. Digital money transfers offer several benefits, including convenience, speed, security, record-keeping, and cost efficiency. Participants will learn about the role of digital money transfers in various scenarios, such as sending money to family or friends, paying for services, receiving pensions or financial support, shopping online, splitting bills with friends, and donating to causes.



[Image by Freepik](#)

They will also understand the basic skills needed for digital money transfers, such as using a mobile device or computer, filling out forms, navigating apps or websites, understanding security steps, checking transaction history, and communicating information clearly.

What is Digital Money Transfer?

A digital money transfer is **a way to send or receive money electronically using mobile apps or online platforms, without needing cash or checks.**

How It Works: You provide details like the recipient's IBAN or username, and the money is transferred securely through your bank or app.



[Image by Freepik](#)

Role of Digital Money Transfers

Digital money transfers revolutionize the way individuals manage their finances by offering secure, efficient, and fast solutions for sending and receiving money. They replace the need for physical cash, reducing the risks of theft or loss, and enable users to perform transactions from the comfort of their homes. Moreover, they provide detailed records for every transaction, ensuring easy tracking and verification for financial accountability.

Examples of Digital Money Transfers

- Sending Money to Family or Friends
- Paying for Services
- Receiving Pension or Financial Support
- Shopping Online
- Splitting Bills with Friends
- Donating to Causes

In this section, focus on:

- **Convenience:** Perform transactions anytime, anywhere.
- **Speed:** Immediate or near-instant money transfers between accounts.
- **Security:** Multi-step authentication and encryption safeguard funds.
- **Record Keeping:** Access detailed transaction histories for better financial management.

Examples of Digital Money Transfers

- Sending Money to Family or Friends
- Paying for Services
- Receiving Pension or Financial Support
- Shopping Online
- Splitting Bills with Friends
- Donating to Causes



[Image by vectorjuice on Freepik](#)

Basic Skills Needed for Digital Money Transfers

- **Using a Mobile Device or Computer:** Know how to operate a smartphone, tablet, or computer for accessing apps or websites.
- **Filling Out Forms:** Enter required details like IBAN, recipient's name, and payment amount accurately.
- **Navigating Apps or Websites:** Learn how to open, log in, and explore money transfer apps or banking websites.
- **Understanding Security Steps:** Use PINs, passwords, and SMS codes for secure transactions.
- **Checking Transaction History:** Locate and review past transactions to confirm payments or receipts.

- Communicating Information Clearly: Provide and request accurate details, such as IBAN or transaction references, to avoid errors.

What Could Go Wrong with Digital Money Transfers?

- Entering Incorrect Information
- Falling for Scams
- Weak Security Practices
- Internet Connectivity Issues
- Using Outdated Apps or Software
- Misunderstanding Fees or Exchange Rates



Image by storyset on Freepik

UNDERSTANDING FORMS AND REQUIRED DATA FIELDS



In this section, participants will learn about the key data fields required for digital money transfers, including IBAN (International Bank Account Number), username or name, phone number, and payment details. They will understand the importance of ensuring accuracy in digital money transfers by double-checking all information, cross-verifying with the recipient, taking their time while entering details, and using auto-fill features carefully. Participants will also learn tips for ensuring accuracy, such as avoiding public Wi-Fi, using secure networks, and reviewing the confirmation screen before submitting a transaction.

confirmation screen before submitting a transaction.

Key Data Fields

- **IBAN (International Bank Account Number)**
 - A unique code that identifies the recipient's bank account.
 - Essential for ensuring the money reaches the correct destination.
- **Username or Name**
 - The name or app username of the person receiving the money.
 - Helps confirm the identity of the recipient.
- **Phone Number**
 - Used for certain payment apps or as an additional verification step
 - Ensures secure and accurate transactions
- **Payment Details**
 - A short note describing the purpose of the transfer (e.g., "Gift for grandson")
 - Helps both sender and recipient keep track of the transaction.

Make sure to keep your focus on the following topics:

- **Key Data Fields:** IBAN, username, phone number, and payment details.

- **Accuracy Tips:** Double-check information, cross-verify with the recipient, and use secure networks.
- **Avoid Public Wi-Fi:** Use secure networks or mobile data to prevent unauthorized access.
- **Review Confirmation Screen:** Check the final summary of the transaction before submitting.

APPS FOR SENDING AND RECEIVING MONEY

This section provides an overview of commonly used apps for sending and receiving money in Romania, such as George by BCR, ING Home'Bank, BT Pay, Revolut, Raiffeisen Smart Mobile, PayPal, and Western Union. Participants will learn how to install and set up these apps, including choosing the right app, downloading it from the App Store or Google Play Store, creating an account, linking their bank account or card, setting up security features, and practicing navigating the app. This comprehensive guide ensures that participants can confidently use these apps for digital money transfers.



Main topics to focus on:

- **Common Apps:** George by BCR, ING Home'Bank, BT Pay, Revolut, Raiffeisen Smart Mobile, PayPal, Western Union.
- **Installation Steps:** Download from App Store or Google Play Store, create an account, link bank account or card.
- **Security Features:** Enable PIN, password, or biometric authentication.
- **Practice Navigation:** Explore the app interface to find features like sending money and viewing transactions.



Install and Set Up Money Transfer Apps

- **Choose the Right App:** Identify which app suits your needs (e.g., Revolut or PayPal, or the app from your bank).
- **Download the App:** Go to the App Store (iPhone) or Google Play Store (Android). Search for the app by name and click "Install."
- **Create an Account:** Open the app and follow the sign-up process.
- Provide details like your name, email, phone number, a secure password or other details provided by the bank. Usually, to setup an internet banking account, you must visit the bank first.

Image by Freepik



Co-funded by the
Erasmus+ Programme
of the European Union

- **Link Your Bank Account or Card:** For some apps, enter your IBAN or card number securely. Complete any verification steps required (e.g., SMS or email code).
- **Set Up Security Features:** Enable PIN, password, or biometric authentication (fingerprint/face recognition). Turn on two-factor authentication for extra protection
- **Practice Navigating the App:** Explore the interface to find features like sending money, viewing transactions, and updating details. Familiarize yourself with help or support options in case of issues.

IDENTIFYING AND AVOIDING COMMON SCAMS

In this section, participants will learn to recognize and avoid common scams, such as phishing attempts. Phishing is a scam where attackers try to trick individuals into sharing personal or financial information through fake messages, emails, or websites. Participants will understand how phishing works, common signs of phishing, and examples of phishing attempts. They will also learn safe sharing practices for sending and receiving money, such as double-checking recipient details, using secure channels, and confirming receipt of funds. Additionally, participants will learn about multi-factor authentication (MFA) as a security method that requires two or more verification steps to confirm their identity during a login or transaction.



[Image by pch.vector on Freepik](#)

What are Phishing Attempts?

Phishing is a scam where attackers try to trick you into sharing personal or financial information through fake messages, emails, or websites.

How It Works:

- Scammers pose as trusted institutions (banks, government agencies, or service providers).
- They send messages asking you to click a link, provide login details, or confirm a transaction.

Common Signs of Phishing

- Urgent language like "Your account will be blocked!"
- Unfamiliar email addresses or phone numbers.
- Poor spelling and grammar in the message.
- Requests for sensitive information like PINs or passwords.
- Suspicious links that don't match the official website.



Co-funded by the
Erasmus+ Programme
of the European Union

Examples of Phishing

- Fake emails pretending to be your bank asking for account verification.
- SMS with a link to "fix" a problem with your account.
- Calls claiming you've won a prize and asking for payment information.

Safe Sharing Practices

For Sending Money

- Double-check recipient details (e.g., IBAN, username) before confirming
- Share only verified and accurate information to avoid errors
- Avoid sharing sensitive details, like passwords or security codes, with others
- Notify the recipient once the transfer is complete to ensure they are informed

For Receiving Money

- Provide clear and correct account details (e.g., IBAN or phone number)
- Use secure channels (trusted apps or official communication) to share account information
- Confirm receipt of funds and notify the sender if any discrepancies occur
- Check transaction notifications and reports to ensure the funds were correctly deposited.



ACCESSING AND UNDERSTANDING TRANSACTION HISTORY

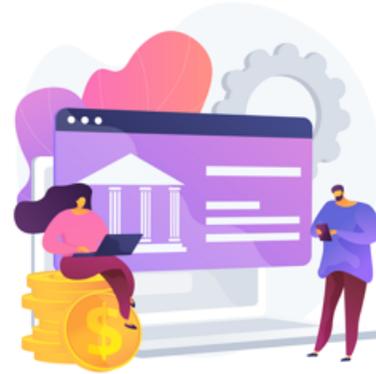
This section teaches participants how to navigate and understand their transaction history. They will learn to log in to their banking app or money transfer platform, locate the transaction section, filter them search, view transaction details, and save records for future use.

Understanding transaction history is important for verifying transactions, providing proof of payment, monitoring spending and income, and resolving errors.

Participants will also engage in activities to identify their IBAN and check their knowledge through quizzes.

Navigate the transaction history (1)

- **Open the App or Website**
 - Log in to your banking app or money transfer platform using your credentials.
 - Locate the Transaction Section: Look for tabs or menus labeled “Transaction History,” “Activity,” or “Payments.” These are often found on the home screen or in the main menu.
- **Filter Your Search**
 - Use available filters like date, amount, or type of transaction to find specific records. For example, select “Sent” or “Received” to narrow down results.



Navigate the transaction history (2)

- **View Details**
 - Click or tap on a transaction to see full details, including sender, amount, and reference number.
 - Verify that the information matches your expectations.
- **Save for Future Use**
 - If needed, download or print the transaction details for personal records or proof of payment.

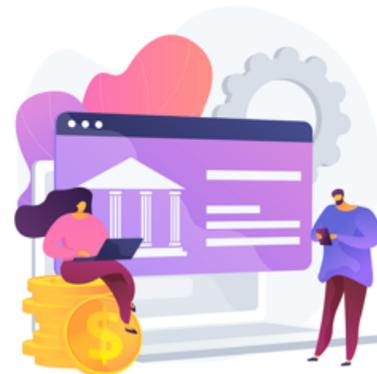


Image by vectorjuice on Freepik

These are the main topics to discuss while presenting this section:

- **Navigation Steps:** Log in, locate transaction section, filter search, view details.
- **Verification:** Confirm payments have been sent or received successfully.
- **Proof of Payment:** Use transaction history as evidence for completed payments.
- **Financial Tracking:** Monitor spending and income to manage budget effectively.

Why is it important?

- **Verification of Transactions**
 - Confirm that payments have been sent or received successfully
- **Proof of Payment**
 - Use transaction history as evidence for completed payments or receipts when needed
- **Financial Tracking**
 - Monitor your spending and income to better manage your budget
- **Error Resolution**
 - Quickly identify discrepancies or unauthorized transactions for prompt resolution.



Co-funded by the
Erasmus+ Programme
of the European Union

ENGAGING ACTIVITIES, YOU CAN ADD

1. **Account Setup Simulation:** Participants simulate setting up an online bank account, including creating a username and password, and verifying identity.
2. **Bank Transfer Relay:** Participants move from station to station, completing steps to make a bank transfer, such as entering recipient details and verifying transaction information.
3. **Role-Playing Scenarios:** Participants practice managing online banking tasks through role-playing scenarios, such as making a transfer or consulting account balance.
4. **Interactive Quiz:** Using a platform like Kahoot! this quiz reinforces knowledge of online banking principles. Participants answer questions in real-time using their devices, and the correct answers are discussed with additional explanations provided as needed.
5. **Secure Transaction Simulation:** This activity involves using the Mobile Money app to simulate making a secure transaction. Participants follow step-by-step instructions to complete a transaction, ensuring they verify details and keep receipts.
6. **Banking Concepts Discussion:** Facilitating a group discussion on basic banking concepts, such as the differences between traditional and online banking, and the advantages and challenges of each.

MODULE 5: USING A CREDIT CARD TO PURCHASE ONLINE GOODS AND SERVICES

This module focuses on teaching participants how to use a credit card to purchase goods and services online. The primary objectives are to develop proficiency in online shopping techniques, enhance awareness of online security, and understand customer rights and ethical practices in online shopping.

OBJECTIVES

- Develop proficiency in online shopping techniques and tools.
- Enhance awareness of online security.
- Understand customer rights and ethical practices in online shopping.



COMPETENCES

Participants will acquire the necessary skills to shop online safely and effectively. They will learn to:

- Navigate e-commerce websites.
- Create and manage online shopping accounts.
- Compare products and prices.
- Understand common online payment methods.
- Communicate with customer service.
- Prevent risks associated with online shopping.
- Manage logistics and track shipments.
- Understand marketing and merchandising insights.
- Integrate technology to enhance the online shopping experience.



TRANSVERSAL COMPETENCES

- **Social Skills:** Enhancing communication and interaction within the group.
- **Trust and Confidence:** Building trust in using online shopping solutions.
- **Financial Literacy:** Understanding financial concepts related to online shopping.
- **Digital Literacy:** Improving overall digital skills and confidence.

METHODOLOGY

The training methodology for this module includes both face-to-face and online training. Face-to-face training involves dialogue, role-playing, and teamwork, while online training includes videos, practical



Co-funded by the
Erasmus+ Programme
of the European Union

exercises, collaborative work, and simulations. This blended approach ensures that participants can engage with the material in various ways, enhancing their learning experience.

TRAINING MATERIALS

- PowerPoint presentations.
- Word handout with practical exercises
- Training mobile app tool.

TOOLS

- **Senior-Friendly Phones/Tablets:** Devices specifically designed for seniors with larger icons, simplified interfaces, and voice commands.
- **Interactive Quiz Platforms:** Tools like Kahoot! for engaging quizzes.
- **Role-Playing Scenarios:** Predefined scenarios for practical exercises.
- **Secure Transaction Simulation:** Mobile Money app for practicing secure transactions.

TRAINING ROADMAP

ACTION 1. Opening

The trainer welcomes back all the participants and invites them to get comfortable for a new training session. He/she summarizes the content of the previous session to help participants remember the key points and after this, the trainer lets the participants know what to expect from this session: duration, main topics, objectives, necessary tools.

ACTION 2. Developing each topic

The training content is divided into several key sections and the trainer presents them as follows:

WEBSITES STRUCTURE AND NAVIGATION

This section introduces participants to the structure of e-commerce websites, which typically include a homepage, menu, and product pages. Participants will learn how to navigate these websites by identifying the menu bar with categories, exploring categories, and using search and filtering options for a more targeted search. They will continue to learn how to browse products by selecting a category, using sub-categories, and exploring product listings.

Structure of e-shop websites

Most e-commerce (e-shop) websites have a simple structure:

- **Homepage:** This is the starting point. It usually features promotions, popular products, and categories.
- **Menu:** It contains links to different product categories.
- **Product Pages:** These provide details about individual items, including pictures, descriptions, prices, and options to add items to your shopping cart.



Image by redgreystock on Freepik

Navigating e-shop websites

Steps for navigation:

- **Identify the menu:** Look for the menu bar with categories.
- **Explore categories:** Click on a category to see sub-categories.
- **Product browsing:** Within each category, scroll through the products or use search and filtering options for a more targeted search.
- **Select a category:** On the website's menu, choose a main category.
- **Use sub-categories:** Within the main category, you'll often find sub-categories. Click on these to narrow down your search.
- **Explore products:** The sub-category will show a list of products. You can scroll through these to find what you're looking for.



Image by pchvector on Freepik



CREATING AND MANAGING ONLINE SHOPPING ACCOUNTS

In this section, participants will learn how to create and manage online shopping accounts. They will understand the process of signing up for an account, filling in personal details, and setting a strong password. Participants will also learn how to log in, update profile settings, and manage their account information, such as shipping address and preferred payment method. Additionally, they will learn how to compare products by checking prices across different websites, evaluating product descriptions, considering brand reputation, and reading customer reviews and ratings.



Co-funded by the
Erasmus+ Programme
of the European Union

Creating an account

For creating an account, you have to:

- **Sign Up:** Look for a "Sign Up" or "Create Account" button on the website.
- **Click on** it to start the registration process.
- **Fill in Details:** Enter your information, such as name, email address, and password. Some websites may require additional details like phone number and address.
- **Set a Strong Password:** Use a combination of letters, numbers, and symbols for security.

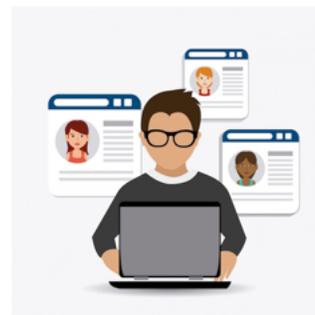


[Image from Freepik](#)

Managing the account

For managing an account, you have to:

- **Logging In:** Use your email and password to log in to the website.
- **Profile Settings:** Within your account, you can update your personal details, such as shipping address, phone number, and preferred payment method.



[Image by studiotock on Freepik](#)



Co-funded by the
Erasmus+ Programme
of the European Union

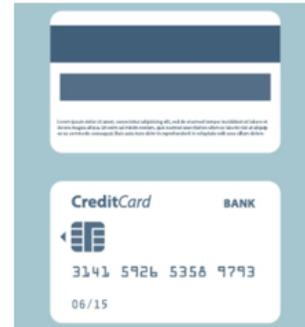
Using a Credit Card for Online Purchases

Shopping online is easy and convenient! Follow these simple steps to use your credit card safely.

Where to Enter Credit Card Details

When you are ready to pay, you will be asked to enter your credit card information:

- **Card Number:** 16-digit number on the front of your card.
- **Expiry Date:** The month and year your card expires (MM/YY).
- **CVV (Security Code):** 3-digit number on the back of your card.



Never sharing credit card details over the phone or email.

Image by [katod](#) on [Freepik](#)

Reviewing the Total Amount

- Before you confirm your purchase with your credit card, always check:
- The price of the item(s).
- Any additional charges like taxes or shipping fees.
- The final total amount before clicking "Place Order" or "Confirm Purchase ,,

Check Your Statements Regularly

- Review your credit card statements for any suspicious charges.
- Report any unauthorized transactions to your bank immediately.

CREDIT AND DEBIT CARDS

How They Work: Enter your card number, expiration date, and security code (CVV) during checkout. Many websites allow you to save card details for future use.

Security Features: Most credit cards offer fraud protection. Look for websites that use SSL (Secure Socket Layer) encryption (indicated by "https" in the URL) to ensure your card details are transmitted securely.

PAYPAL

How It Works: PayPal acts as a trader between your bank or card and the seller. You only need to enter your PayPal login and password to make a payment.

Security Features: PayPal keeps your card and bank information secure by not sharing them with sellers. It also offers purchase protection, which can refund you if there's an issue with your order.



Co-funded by the
Erasmus+ Programme
of the European Union

DIGITAL WALLETS (e.g. Apple Pay, Google Pay)

How They Work: Store your card information in a digital wallet on your smartphone. During checkout, you can use the wallet to pay with a single tap.

Security Features: Digital wallets use tokenization (replacing card details with a unique identifier) and biometric authentication (fingerprint, facial recognition) to secure transactions.

OTHER WAYS OF PAYMENTS

Bank Transfers

- Some websites allow you to pay directly from your bank account.
- You may need to enter **your online banking details** to complete the purchase.
- Only use this on **trusted websites**.

Buy Now, Pay Later (Afterpay, Klarna)

- Let's you buy something now and pay in small amounts over time.
- You may need to sign up and link your card or bank account.
- Be sure to pay on time to avoid extra charges.
- **Gift Cards & Store Credit**
- Some websites let you pay with a **gift card or store credit**.
- Enter the **gift card number and PIN** at checkout



Image by Freepik

LATEST TREND: PAYMENT VIA POS AT EASYBOX

- **How to Pay:** At the Easybox, use your debit or credit card to make a payment directly at the Point of Sale (POS) terminal. Simply insert, swipe, or tap your card, and follow the prompts on the screen.

- **Confirm Payment:** After entering your payment details, the system will confirm your transaction with a receipt. Make sure to keep the receipt as proof of your payment.

RISK PREVENTION SKILLS FOR SAFE ONLINE SHOPPING

In this section, participants will learn essential risk prevention skills to ensure safe online shopping. They will understand how to set privacy parameters by limiting the information shared, adjusting privacy settings on web browsers and shopping apps, and unsubscribing from unwanted newsletters. Participants will also learn how to communicate with customer service effectively, describe issues clearly, and know their desired outcome. Additionally, they will understand logistical skills for managing shipping methods, tracking shipments, and interpreting tracking information.

Recognize and avoid scams

- ✓ **Check Website Legitimacy** – Look for “https://” and a **padlock** in the web address. Avoid unknown sites with poor design or too-good-to-be-true deals.
- ✓ **Beware of Phishing Emails & Calls** – Never click on suspicious links in emails or text messages asking for personal details. “Unsubscribe,, from unwanted newsletters.
- ✓ **Avoid Fake Sellers** – Read product reviews and check seller ratings before making a purchase.
- ✓ **Use an alias email for shopping** – Consider using a separate email address solely for online shopping. This helps keep your primary email private and reduces the risk of phishing attacks.



Image by vectorjuice on Freepik

Protect personal and payment information

- ✓ **Use Strong Passwords** – Create unique passwords with a mix of letters, numbers, and symbols. Avoid using personal details like birth dates.
- ✓ **Never Share Credit Card Details** – Legitimate companies will never ask for card details via phone, email, or text.
- ✓ **Enable Two-Step Verification** – Add an extra layer of security by using a code sent to your phone when logging in.



Image by vectorjuice on Freepik

Verify website security and purchase safely

- **Check for Secure Payment Methods** – Use trusted payment options like credit cards, PayPal, or digital wallets instead of direct bank transfers.
- **Review Return Policies** – Read return and refund policies before purchasing to avoid issues with faulty or incorrect items.
- **Monitor Your Bank Statements** – Regularly check your credit card or bank statements for unauthorized transactions and report suspicious activity immediately.

Marketing and merchandising insights

How to compare products

Price comparison:

- When looking at products, check their prices across different websites or apps. Some online stores may have discounts or promotions that others do not.
- Use price comparison websites or browser extensions (e.g. Google Shopping) to view prices for the same product from various sellers. This can help you find the lowest price.

Quality evaluation:

- Product descriptions: Read the product details provided on the website, including specifications, materials, and features.
- Brand reputation: Consider the brand's reputation. Well-known brands often have higher quality standards. Check if the brand has official websites or social media pages for more information about their products.

Understanding reviews and ratings

- Look at customer reviews on the product page. Reviews provide insights into the real-life experiences of people who have already used the product.
- Ratings: Most products have a star rating system (e.g., out of 5 stars). A higher average rating generally indicates a better product.
- Focus on both positive and negative reviews to get a balanced understanding of the product's pros and cons.

Finding discounts

- Keep an eye out for promotions like "Black Friday," or end-of-season sales. Many websites offer significant discounts during these periods.
- Subscribe to newsletters from online stores to receive updates on upcoming sales and exclusive discount codes.

The common types of discounts are:

- Percentage off
- Fixed amount off
- Buy one get one free
- Free shipping
- Coupons and promo codes
- Coupons
- Promo codes
- Sales events
- Bundle deals

[Image by Freepik](#)





Co-funded by the
Erasmus+ Programme
of the European Union

Other types of benefits

- Loyalty programs
- Points-based programs
- Membership and subscription services
- Common marketing strategies
- Limited-time offers
- Personalized recommendations
- Free shipping thresholds
- Email newsletters and notifications
- Social media and influencer marketing

Managing a budget

Managing a budget for online shopping tracking expenses and avoiding overspending.

✓ Creating and sticking to a budget is crucial for responsible online shopping. This involves setting spending limits, tracking purchases, and making informed decisions to avoid impulse buying.

✓ How to manage your online shopping budget:

- set a monthly or weekly budget
- track your expenses
- avoid impulse buying
- use alerts and notifications
- understanding various online payment methods and their security features

Understanding shipping goods and tracking orders

Common shipping methods

- Standard Shipping: A regular, cost-effective shipping option with a longer delivery time, typically 5-7 business days.
- Expedited Shipping: Faster than standard shipping, delivering within 2-3 business days, usually at a higher cost.
- Overnight Shipping: Delivers the next day, offering the fastest service for urgent shipments, but often more expensive.
- Two-Day Shipping: Guarantees delivery within two business days, often available for a premium fee.
- International Shipping: Ships products to other countries, which may take several days or weeks depending on the destination.
- Flat Rate Shipping: A shipping option where the cost stays the same regardless of the weight or size of the item, as long as it fits within the provided packaging.

- **Free Shipping:** Often offered as a promotion, where the seller absorbs the shipping cost, usually with a minimum purchase requirement.

How to track your shipment

- Get the tracking number
- Visit the shipping carrier's website
- Use the retailer's tracking feature
- Enable notifications

Interpreting tracking information:

- In transit
- Out for delivery
- Delivered



Image by rawpixel on Freepik

Resolving shipping issues

- **Check the tracking information:** Use your tracking number to verify the status of your order. Learn how to identify if there's been a delay or change in delivery date.

- **Contact the carrier for updates:** If there's a delay, contact the shipping carrier (e.g., UPS, FedEx) to get more detailed information and resolve any delivery issues.

- **Reach out to customer service:** Learn how to effectively contact the retailer's customer service to report problems like missing or damaged items and get a quick solution.

Legal and ethical awareness

Legal awareness

- Key consumer rights
- Right to information
- Right to cancel (Cooling-Off Period)
- Right to a refund
- Right to data privacy
- Right to secure transactions

Ethical considerations

- Supporting fair-trade products
- Choosing sustainable brands
- Avoiding fast fashion
- Considering animal welfare
- Recognizing greenwashing

How to communicate with customer service

Contact customer service

Find customer support contact options, most online stores offer multiple ways to contact customer service, including:

- **Live chat:** Typically found on the website or app for instant messaging with a representative.
- **Email:** Use the website's "Contact Us" section to find the customer support email address.
- **Phone support:** Some stores provide a phone number for direct contact.
- **Social media:** Some companies offer support through their social media accounts (e.g., Facebook, Twitter).



Image by Freepik

DESCRIBE YOUR ISSUE CLEARLY!

Be specific: When contacting customer service, explain your problem in detail. Include relevant information like:

- Order number
- Product name and description
- Date of purchase
- A clear explanation of the issue (e.g., "The product arrived damaged," "Received the wrong size")

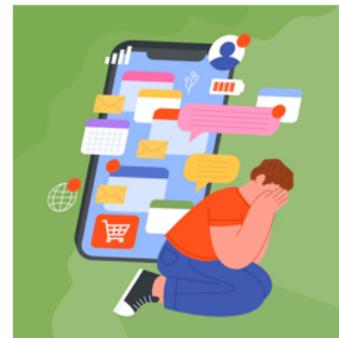


Image by Freepik

Know your desired outcome

Before contacting customer support, decide what you want as a resolution. Common options include:

- A refund
- A replacement product
- Store credit
- Return instructions



Image by vectorjuice on Freepik



Co-funded by the
Erasmus+ Programme
of the European Union

Refund methods

Understand how the store processes refunds.

Common options include:

- Original payment method: The refund will go back to your credit card, PayPal, or bank account.
- Store credit: Some stores only offer store credit instead of a direct refund.

Engaging activities, you can add

- **Account Setup Simulation:** Participants simulate setting up an online bank account, including creating a username and password, and verifying identity.
- **Bank Transfer Relay:** Participants move from station to station, completing steps to make a bank transfer, such as entering recipient details and verifying transaction information.
 - **Role-Playing Scenarios:** Participants practice managing online banking tasks through role-playing scenarios, such as making a transfer or consulting account balance.
 - **Interactive Quiz:** Using a platform like Kahoot! this quiz reinforces knowledge of online banking principles. Participants answer questions in real-time using their devices, and the correct answers are discussed with additional explanations provided as needed.
 - **Secure Transaction Simulation:** This activity involves using the Mobile Money app to simulate making a secure transaction. Participants follow step-by-step instructions to complete a transaction, ensuring they verify details and keep receipts.
 - **Banking Concepts Discussion:** Facilitating a group discussion on basic banking concepts, such as the differences between traditional and online banking, and the advantages and challenges of each.

Action 3. Debriefing and Closure

The trainer summarizes the content of the session and clarifies possible doubts and questions. The trainer explains the activities to be done in the next online training session.

MODULE 6: PROCESSING ONLINE PAYMENTS FOR TAXES AND BILLS

This module focuses on teaching participants how to process online payments for taxes and bills. The primary objectives are to provide a clear understanding of online payment systems and develop the practical skills needed to navigate and use online payment portals for taxes and bills.

OBJECTIVES

- Provide a clear understanding of online payment systems.
- Develop practical skills to navigate and use online payment portals for taxes and bills.



COMPETENCES

Participants will acquire the necessary skills to process online payments confidently. They will learn to:

- Understand how online payments work, including different payment methods.
- Navigate online payment portals (e.g., government tax sites, utility company sites).
- Make online payments.
- Handle taxes online and understand tax portals.



TRANSVERSAL COMPETENCES

- **Social Skills:** Enhancing communication and interaction within the group.
- **Trust and Confidence:** Building trust in using online payment solutions.
- **Financial Literacy:** Understanding financial concepts related to online payments.
- **Digital Literacy:** Improving overall digital skills and confidence.

METHODOLOGY

The training methodology for this module includes both face-to-face and online training. Face-to-face training involves dialogue, role-playing, and teamwork, while online training includes videos, practical exercises, collaborative work, and simulations. This blended approach ensures that participants can engage with the material in various ways, enhancing their learning experience.



Co-funded by the
Erasmus+ Programme
of the European Union

TRAINING MATERIALS

- PowerPoint presentations.
- Word handouts with practical exercises
- Training mobile app tool.
- Videos and scenarios for practical exercises.

TOOLS

- **Senior-Friendly Phones/Tablets:** Devices specifically designed for seniors with larger icons, simplified interfaces, and voice commands.
- **Interactive Quiz Platforms:** Tools like Kahoot! for engaging quizzes.
- **Role-Playing Scenarios:** Predefined scenarios for practical exercises.
- **Secure Transaction Simulation:** Mobile Money app for practicing secure transactions.

TRAINING ROADMAP

ACTION 1. Opening

The trainer welcomes back all the participants and invites them to get comfortable for a new training session. He/she summarizes the content of the previous session to help participants remember the key points and after this, the trainer lets the participants know what to expect from this session: duration, main topics, objectives, necessary tools.

ACTION 2. Developing each topic

The training content is divided into several key sections and the trainer presents them as follows:

UNDERSTANDING ONLINE PAYMENT PORTALS

This section introduces participants to online payment portals, which are secure websites or apps where users can pay for goods and services directly from their mobile phones or other digital devices. Participants will learn about different types of online payment portals, including government sites for paying taxes, fines, or other official fees, and utility sites for paying bills like electricity, water, and gas.

They will also learn how to access these portals by opening their phone's web browser, typing the website address, and using their login details or following the registration process to create an account.



Co-funded by the Erasmus+ Programme of the European Union

Main topics of this section:

- **Types of Portals:** Government sites for taxes and fines, utility sites for bills.
- **Accessing Portals:** Open browser, enter website address, log in or register.
- **Secure Websites:** Ensure the portal is secure before entering personal information.
- **Examples:** Property tax, income tax, electricity, water, gas bills.



Image by storyset on Freepik

Online Taxes Examples

Income Tax - Pay income taxes easily through secure websites. You can use your bank account, credit/debit cards, or even digital wallets to make payments. Help is often available if you need assistance filing or paying.

Property Tax - Many local governments allow you to pay your property taxes online. Payments are based on the value of your property (house, car, land) and you can often choose to pay in installments. You can track your payments and set reminders to avoid missing due dates.

Get familiar with Utility Payment Portals

Understanding Utility Payment Portals

What Are Utility Portals?

- Secure online platforms where you can pay for services like electricity, water, gas, internet, and phone bills.
- Accessible via official websites or mobile apps.

Features of Utility Portals

- **Bill Tracking:** View past and upcoming bills in one place.
- **Usage Monitoring:** Track energy, water, or internet usage.
- **Alerts and Reminders:** Get notifications for due dates and payments.
- **Downloadable Receipts:** Keep digital records for future reference.



Image by gstudioimagen on Freepik

Understanding Utility Payment Portals

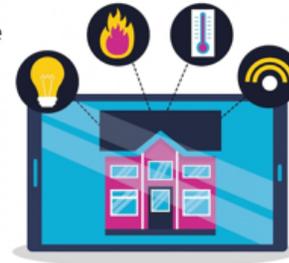
In this section, participants will learn what online payments are and how they allow users to pay bills or make purchases electronically without needing to go to a physical location. They will understand the steps for making online payments, including logging into a payment portal, entering payment details,

selecting payment methods, confirming the payment, and saving receipts. Participants will also learn about scheduling recurring payments for regular bills.

Understanding Utility Payment Portals

What Are Utility Portals?

- Secure online platforms where you can pay for services like electricity, water, gas, internet, and phone bills.
- Accessible via official websites or mobile apps.



Features of Utility Portals

- **Bill Tracking:** View past and upcoming bills in one place.
- **Usage Monitoring:** Track energy, water, or internet usage.
- **Alerts and Reminders:** Get notifications for due dates and payments.
- **Downloadable Receipts:** Keep digital records for future reference.



Image by pstudioimagen on Freepik

Types of Utilities Paid Online

This section provides an overview of tax portals, which are official websites provided by national or local tax authorities where taxpayers can file their tax returns, make payments, and manage their tax accounts.

Participants will learn about different types of tax portals, including national tax portals for filing income taxes and local tax portals for regional taxes. They will also learn how to access these portals, fill out tax returns, and make tax payments online using various payment methods.

Types of Utilities Paid Online

- **Electricity Bills** - Pay for household or business electricity usage. Some portals offer energy-saving tips and usage reports.
- **Water Bills** - Manage and pay water service fees for your home or business. View detailed usage reports to track consumption.
- **Gas Bills** - Pay for natural gas supply used for heating and cooking. Some providers offer budget plans to spread payments over time.
- **Internet and Cable Bills** - Pay for broadband, fiber, or cable TV services online. Options for upgrading plans or changing services directly through the portal.
- **Phone Bills (Landline & Mobile)** - Easily pay for mobile and home phone services. Set up auto-pay to avoid service interruptions.
- **Waste Management Bills** - Pay for garbage collection and recycling services. Some portals allow scheduling bulk pickups or additional services.



Image by storyset on Freepik





Co-funded by the
Erasmus+ Programme
of the European Union

Navigating Tax and Utility Payment Portals

Navigating steps

An online payment portal is a secure platform, accessible via a website or app, that allows users to pay taxes and services directly from their mobile phones or other digital devices.

- Locate the Login Section – Find and enter your credentials on the official government or utility website.
- Explore the Main Menu – Identify key sections such as "Payments," "Billing," "Account Settings," and "Support,"
- Access Transaction History – Navigate to the payment history or billing section to review past transactions and receipts.
- Find Support and Help Features – Locate FAQs, chat support, or customer service contact details for assistance.

Setting Up and Managing Your Account

Setting Up and Managing Your Account

- **Visit the Official Website** – Go to the government or utility provider's official website and look for the "Sign Up" or "Register" option.
- **Create an Account** – Enter your personal details (name, email, phone number) and set a strong password.
- **Verify Your Identity** – Complete any verification steps, such as email confirmation, phone OTP (One-Time Password), or security questions.
- **Link a Payment Method** – Add a bank account, debit/credit card, or set up an online wallet for transactions.
- **Set Up Security Features** – Enable two-factor authentication (2FA), set up alerts for transactions, and use strong passwords.
- **Manage Account Preferences** – Update contact details, set up auto-pay if you want, and customize notification settings for payment reminders.
- **Test Your Account** – Make a small payment or check your billing details to ensure everything is set up correctly.



[Image by vectorjuice on Freepik](#)





Co-funded by the
Erasmus+ Programme
of the European Union

Making Secure Online Transactions BENEFITS

Convenient and Secure: Pay bills, make purchases, and manage finances online without needing to visit physical locations.

Encrypted and Secure Portals: Payments are processed through secure, encrypted websites or mobile apps.

Multiple Payment Options: Link bank accounts, credit/debit cards, or digital wallets for quick transactions.

Automatic Payments: Set up recurring payments for added convenience.

Transaction Tracking: Keep track of transactions and digital receipts for easy management.

Hassle-Free Experience: Enjoy a smooth, efficient payment process.



Examples:

- Paying utility bills (electricity, water, gas).
- Subscriptions (TV, internet, streaming services).
- Insurance payments, loans, or credit card bills.



[Image by vectorjuice on Freepik](#)

Making Secure Online Transactions MAIN STEPS

- **Log in to the Official Website** – Ensure you are on the correct government or utility website (check for "https://" and official domains).
- **Navigate to the Payment Section** – Locate the "Pay Bill," "Make a Payment," or "Billing" tab on the website.
- **Select Payment Method**
 - Credit/Debit Card: enter your card number, expiry date, security code (CVV), and billing address.
 - Bank transfer: provide your bank account number and routing number to complete a direct payment from your bank.
 - Mobile Money (if available): input your mobile money account number and confirm the transaction via your phone.
- **Enter Payment Details** – Input the amount, billing period, and any required reference numbers.
- **Verify Transaction Details** – Double-check the payment summary for accuracy before proceeding.
- **Confirm and Complete Payment** – Submit the payment and wait for a confirmation message or email receipt.





Co-funded by the
Erasmus+ Programme
of the European Union

Downloading and storing receipts

- **Download the receipt:**
 - After submitting your tax return or payment, the portal will usually provide an option to download a PDF receipt or email you a copy.
 - Click on the “Download Receipt” button and save the file to your computer or mobile device.
- **Email confirmation:**
 - Most tax portals will automatically send a confirmation email with a digital copy of your receipt. Be sure to check your inbox and save this email for your records.



[Image by storyset on Freepik](#)



Monitor for Fraud or Errors

1. Recognizing Payment Errors

Double Charges: Check for duplicate transactions in your payment history.

Incorrect Amounts: Ensure the billed amount matches your actual usage.

Failed Transactions: If a payment fails, confirm it wasn't deducted from your account before retrying.

2. Identifying Fraudulent Activity

Unauthorized Transactions: Regularly review statements for any unfamiliar charges.

Phishing Scams: Avoid clicking on suspicious emails or links pretending to be from utility providers.

Fake Websites: Always use the official website or app to make payments.

3. Protecting Your Information

Enable Alerts: Set up email or SMS notifications for transactions.

Use Secure Connections: Avoid making payments on public Wi-Fi networks.

Two-Factor Authentication (2FA): Add extra security by requiring a code in addition to your password.

4. Steps to Take If You Spot an Issue

Report Suspicious Transactions: Contact your utility provider or bank immediately.

Request a Refund: If an error occurs, check the portal for dispute options.

Update Your Credentials: Change passwords if you suspect unauthorized access.



Co-funded by the
Erasmus+ Programme
of the European Union

ENGAGING ACTIVITIES, YOU CAN ADD

1. **Portal Navigation Simulation:** Participants simulate navigating an online payment portal, including logging in, entering payment details, and confirming payments.
2. **Tax Return Relay:** Participants move from station to station, completing steps to fill out and submit a tax return, such as entering personal details and income information.
3. **Role-Playing Scenarios:** Participants practice handling online payments and tax returns through role-playing scenarios, such as making a payment or resolving a payment issue.
4. **Interactive Quiz:** Using a platform like Kahoot! this quiz reinforces knowledge of online payment systems. Participants answer questions in real-time using their devices, and the correct answers are discussed with additional explanations provided as needed.
5. **Receipt Management Exercise:** Participants practice downloading, saving, and organizing digital receipts, ensuring they understand the importance of record-keeping.

Action 3. Debriefing and Closure

The trainer summarizes the content of the session, and the main topics discussed during the training. He/she clarifies possible doubts and questions, offers support to the participants who still might have technical difficulties. The trainer gives out feedback forms and asks the participants what their feelings are now, at the end of the training and how they intend to use the learned information in the future.

Action 4. Survey on acquired knowledge- Knowledge evaluation T6

The trainer will apply the knowledge verification questionnaire that was used in Module 1 to assess the progress made by the trainees after completing all six modules.



FINAL THOUGHTS

By completing these modules, participants will be well-equipped to navigate the digital financial world with confidence and security. The combination of theoretical knowledge and practical exercises ensures a comprehensive learning experience, empowering participants to manage their finances digitally. Trainers are encouraged to use the provided materials and activities to create an engaging and supportive learning environment, fostering trust and confidence in digital financial solutions.

Techniques to Implement the Modules More Effectively

- 1. Interactive Learning:** Incorporate interactive elements such as quizzes, simulations, and role-playing scenarios to keep participants engaged. Tools like Kahoot! can be used for real-time quizzes, while role-playing exercises can help participants practice real-world scenarios.
- 2. Blended Learning Approach:** Utilize a mix of face-to-face and online training to cater to different learning preferences. Face-to-face sessions can focus on discussions and hands-on activities, while online sessions can include videos, practical exercises, and collaborative work.
- 3. Personalized Feedback:** Provide personalized feedback to participants during and after activities. This helps them understand their strengths and areas for improvement, enhancing their learning experience.
- 4. Real-World Examples:** Use real-world examples and case studies to illustrate key concepts. This makes the material more relatable and helps participants understand how to apply what they've learned in their daily lives.
- 5. Group Activities:** Encourage group activities and discussions to foster collaboration and peer learning. Group work can help participants learn from each other's experiences and perspectives.
- 6. Regular Assessments:** Conduct regular assessments to gauge participants' understanding and retention of the material. This can include quizzes, practical exercises, and group discussions.
- 7. Supportive Environment:** Create a supportive and inclusive learning environment where participants feel comfortable asking questions and sharing their experiences. This can enhance their confidence and engagement.
- 8. Follow-Up Sessions:** Schedule follow-up sessions to reinforce learning and address any questions or challenges participants may have encountered. This helps ensure long-term retention and application of the material.

By implementing these techniques, trainers can enhance the effectiveness of the modules, ensuring that participants not only learn the essential skills but also feel confident in applying them in their daily lives. This comprehensive approach will help build a strong foundation of digital financial literacy, empowering participants to navigate the digital financial landscape with ease and security.

BIBLIOGRAPHY

- <https://www.digitaltrends.com/mobile/guide-to-android/>
- <https://edu.gcfglobal.org/en/androidbasics/getting-started-with-your-device/1/>
- <https://edu.gcfglobal.org/en/androidbasics/>
- <https://support.google.com/android/answer/12761388?sjid=2735699982701396101-EU&hl=en>
- <https://guidebooks.google.com/android/getstarted>
- <https://guidebooks.google.com/android/getstarted/gesturenavigation?hl=en&sjid=2735699982701396101-EU>
- <https://guidebooks.google.com/android/getstarted>
- <https://guidebooks.google.com/get-started-with-google>
- <https://guidebooks.google.com/get-started-with-google/get-started/icons-on-your-phone>
- <https://guidebooks.google.com/get-started-with-google/get-started/how-to-get-around-on-your-phone>
- <https://guidebooks.google.com/online-security>
- <https://guidebooks.google.com/android/usetheappsonyourphone/addapaymentmethodtogoogleplay>
- <https://guidebooks.google.com/android/usetheappsonyourphone/protectyourgoogleplaypurchases>
- Send an e-mail
- https://support.google.com/mail/answer/2819488?hl=en&ref_topic=3395756&sjid=2735699982701396101-EU
- Add attachment
- https://support.google.com/mail/topic/7280128?hl=en&ref_topic=3394151&sjid=2735699982701396101-EU
- https://support.google.com/mail/answer/6584?hl=en&ref_topic=7280128&sjid=2735699982701396101-EU
- Send an e-mail and attachments confidentially
- https://support.google.com/mail/answer/7674059?hl=en&ref_topic=3395756&sjid=2735699982701396101-EU
- Reply to e-mail
- https://support.google.com/mail/answer/6585?hl=en&ref_topic=3395756&sjid=2735699982701396101-EU
- Read
- https://support.google.com/mail/topic/3394652?hl=en&ref_topic=3394150&sjid=2735699982701396101-EU
- Open & download attachments in Gmail
- https://support.google.com/mail/topic/3394652?hl=en&ref_topic=3394150&sjid=2735699982701396101-EU
- CFPB (Consumer Financial Protection Bureau). Managing Credit Cards and Digital Wallets Safely: A Guide for Consumers. CFPB, 2020.
- Chaffey, Dave. Digital Business and E-Commerce Management: Strategy, Implementation, and Practice. Pearson, 2019.
- Chen, Jie, și Hsin-Yu Shih. E-Commerce Product Analysis: A Guide for Comparing Prices and Quality Online. Springer, 2021.



Co-funded by the
Erasmus+ Programme
of the European Union

- Choi, Chul Ho, și Ana S. Perea y Monsuwé. Influence of Social Media and Digital Marketing on Consumer Buying Behavior. IGI Global, 2020.
- Dimoka, Angelika, et al. Consumer Information Processing in E-Commerce: The Impact of Online Reviews and Recommendations. MIT Press, 2019.
- Easttom, Chuck. Cybersecurity: An Introduction for Beginners and Intermediates. Jones & Bartlett Learning, 2018.
- European Consumer Centre Network. The European Consumer Centres Network (ECC-Net): Your Rights When Shopping Online in the EU. ECC-Net, 2020. Disponibil online: <https://www.eccromania.ro>
- Garfinkel, Simson, și Gene Spafford. Web Security, Privacy, and Commerce. O'Reilly Media, 2011.
- Hunt, Troy. Pwned: Password Security and the Future of Identity Verification. Independently published, 2020.
- Kaspersky Lab. Cybersecurity Awareness for Online Shoppers: A Guide to Safe E-Commerce Practices. Kaspersky, 2020.
- Kotler, Philip, și Kevin Lane Keller. Marketing Management. Pearson, 2016. (cu accent pe strategii de marketing, promoții și loializarea clienților)
- Laudon, Kenneth C., și Carol Guercio Traver. E-Commerce 2020: Business, Technology, Society. Pearson, 2020.
- Nehf, James P. Consumer Protection in the Age of the 'Information Economy': A Guide for Digital Consumers. Cambridge University Press, 2015.
- NIST. Digital Identity Guidelines: Authentication and Lifecycle Management. NIST Special Publication 800-63B, 2020. Disponibil online: <https://www.nist.gov>
- OECD. Protecting Consumers in E-commerce: OECD Guidelines. OECD Publishing, 2016.
- OECD/INFE. Financial Education and Consumer Protection: Digital Payment Systems and the Impact on Financial Literacy. OECD Publishing, 2019.
- Schneier, Bruce. Secrets and Lies: Digital Security in a Networked World. Wiley, 2015.
- Singh, Sujeet. Digital Payment Solutions and Cybersecurity: Practical Guidelines. Academic Press, 2022.
- Solomon, Michael R., și Nancy J. Rabolt. Consumer Behavior: In Fashion and Marketing. Pearson, 2019. (abordează tehnici de marketing, strategii de vânzare și influența acestora asupra consumatorilor)
- Statista. E-commerce in Europe: Market Trends and Digital Transformation. Statista Reports, 2021.
- Tuten, Tracy L., și Michael R. Solomon. Social Media Marketing. Sage Publications, 2020. (include aspecte despre recenzii online și influența lor asupra deciziilor de cumpărare)
- Government of Romania - National Payment Portal, available at: <https://www.ghiseul.ro>
- National Agency for Fiscal Administration (ANAF), available at <https://www.anaf.ro>
- National Bank of Romania - Electronic Payments Guide, available at <https://www.bnr.ro>
- European Union Directives on Electronic Payments, Regulation (EU) 2015/751 and Directive (EU) 2015/2366 (PSD2), available at <https://eur-lex.europa.eu>