1

2

3

4

5

6

MOBILE MONEY

Module 2
Security & Prevention

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project number: 2023-1-RO01-KA220-ADU-000157797

MOBILE MONEY

Partners

Asociatia Four Change, Romania

Zavod IZRIIS, Slovenia

E-SENIORS: INITIATION DES SENIORS AUXNTIC ASSOCIATION, France

GUnet, Greece

Asociatia Niciodata Singur – Prietenii Varstnicilor, Romania

Fundació Gesmed Fundació de la Comunitat Valenciana, Spain

Co-funded by the European Union

Modules

1. Basic digital literacy skills

2. Security & Prevention

3. Managing a bank account online

4.. Online solutions for receiving and sending money

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

6. Processing online payments for taxes and bills

Co-funded by
the European Union

Unit 1

Introduction

Objectives

On completion of this unit, you will be informed about

✓The learning objectives and training content of this module

✓The training methodology used and the duration of this module

Image by vectorjuice on Freepik

Co-funded by the European Union

Competences

After completing this module, you will:

- Acquire the skills necessary to use mobile money solutions safely and confidently:
  - ✓ Understand what online security is.
  - ✓ Understand what is personal and sensitive data.
  - ✓ Understand the concepts of privacy and security.
  - ✓ Know what email spamming and phishing are and how to respond to them
  - ✓ Know the criteria for deciding which links are safe to visit
  - ✓ Know your online rights
  - ✓ Understand what GDPR is and why we need it
  - ✓ Know how to apply security and preventative measures

Co-funded by the European Union

Training content

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

Co-funded by the European Union

Training methodology and duration

Duration: 4 hours

- Face to face session:2 hours
- Online training: 2 hours

Methodology

- Active and participative
- Face to face training:
  - ✓Dialogue ✓ Role playing ✓ Teamwork
- Online training:
  - ✓Selected or own produced videos
  - ✓Practical implementation of some tips agreed in the classroom
  - ✓Some collaborative work
  - ✓Simulation

Co-funded by
the European Union

Unit 2

Online Safety and Personal Data

Objectives

On completion of this unit, you will know:

✓What is online safety

✓What is personal data and examples of them

Image by vectorjuice on Freepik

Co-funded by the European Union

Online Safety

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.

It is therefore of the utmost importance for Internet users to take steps to:

- Protect of their **sensitive personal data;**
- Use online tools and services, such as, data encryption, that **ensure the privacy and security** of their customers’ information when communicating with them online.

What is Personal Data?

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

Various pieces of information that together can be used to **identify a specific individual**, are also personal data.

Image by storyset on Freepik

Examples of Personal Data

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;
- 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.

Unit 3

Sensitive data, privacy and security

Objectives

On completion you will know:

✓ What personal data is considered sensitive.

✓ What is sensitive personal and financial data.

✓ Understand the concepts of privacy and security

✓ What is online privacy and how to be secure online

Image by vectorjuice on Freepik

Co-funded by the European Union

What Personal Data is considered sensitive?

Sensitive personal data

The following personal data are considered ‘**sensitive**’ and are subject to specific processing conditions:

- Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
- Photos, videos;
- Trade union membership;
- Genetic data, biometric data processed solely for the purpose of identification of a human being;
- Data concerning health;
- Data concerning the sex life or sexual orientation of a person.

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

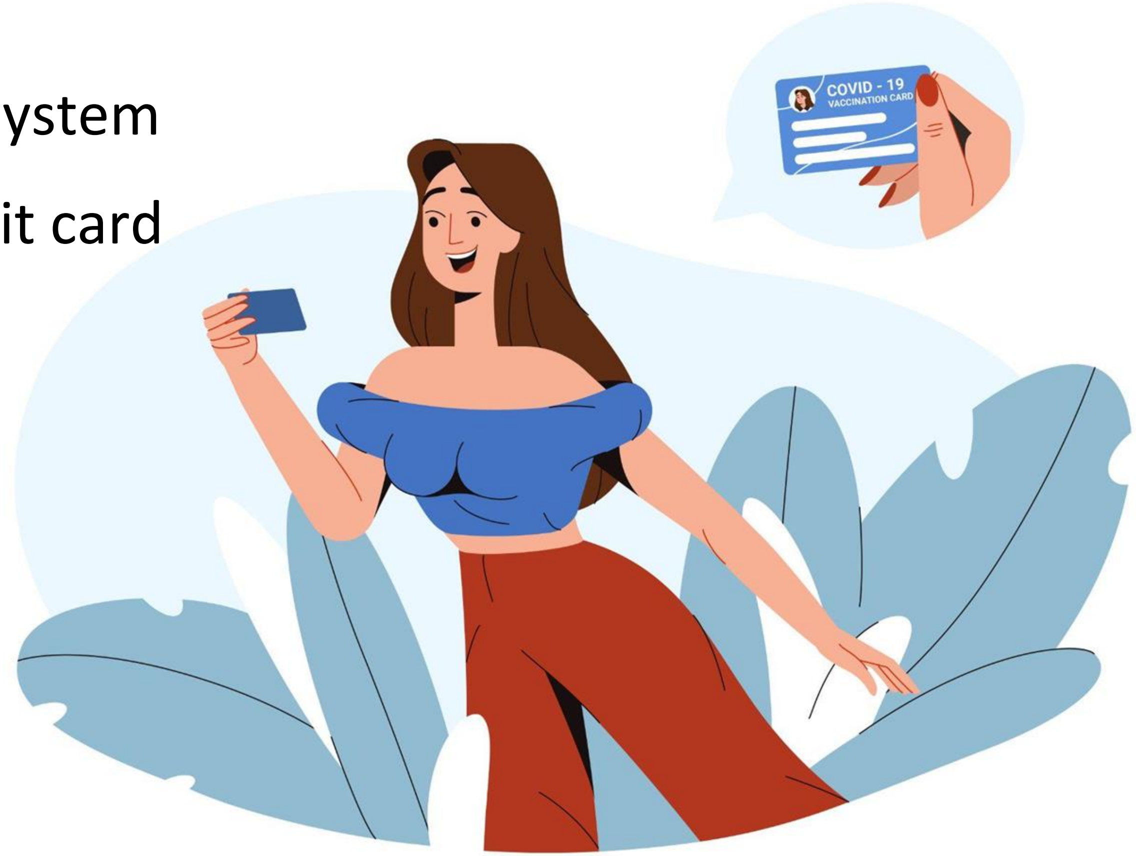


Image by redgreystock on Freepik

What is Privacy?

Privacy is about:

- How we **control our personal data,** and
- how **they are used** by the third parties who have received it, in a secure manner.

Think about the **privacy policies** you're asked to read and agree to when you visit a website or download a new smartphone app.

Image by storyset on Freepik

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

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 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.

Unit 3

Spam and phishing

Objectives

On completion you will know:

✓ What is spam and phishing

✓ How to identifying spam

✓ When a link is safe to visit

Image by vectorjuice on Freepik

Co-funded by the European Union

What is 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.

Image by vectorjuice on Freepik

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

What to do or not to do?

- ✓ 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.

Activity: Is the link safe to visit?

Decide, if the link is safe to visit:

Suppose you receive an email from a bank asking you to click on a link like the one below, and submit personal data, such as username, passwords, and credit card details.

http://url5423.eka.de/ls/click?upn=V1OaWNMSPs2Lb0JqHpnyTLRlk2703ToIFpo2vd2M
2FnC6T5iVsCdbcug7l6pkTad-2FBfACSlC-2BKw-3D-3DhmuAs-OaWNMSPs2Lb0JqHpn-asl

1. *Do not hurry, think twice, and decide if this link is safe to visit.*
2. *Think about the reasons.*

Image by pch.vector on Freepik

Image by freepik

Activity: Is the link safe to visit? (2)

The answer. *This link* is **not secure** for a number of reasons:

- It uses http instead of https.
- The domain name is not related to the official name of the bank.
- The link is suspiciously long.
- The domain name of the link is different from the domain name of the sender's email address.
- A real bank will never ask for usernames, passwords or credit card details.

Image by pch.vector on Freepik

Unit 4

What are your online rights

Objectives

On completion you will know:

✓ What are your digital rights and obligations

✓ What is GDPR and why do we need it

Image by vectorjuice on Freepik

Co-funded by the European Union

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 ana responsible digital environment for all.

We are all now connected

by the Internet, like neurons in

a giant brain.

Stephen Hawking

Image by storyset on Freepik

What is GDPR and who needs to comply with it?

What is GDPR?

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

Who must comply with GDPR?

- Any organization that processes personal data of individuals in the EU must comply with the GDPR.
- “**Processing**” is a broad term that covers just about anything you can do with data: collection, storage, transmission, analysis, etc.
- “**Personal data**” is any information that relates to a person, such as names, email addresses, IP addresses, eye color, political beliefs, and etc.

Source | Pixabay license

Who needs to comply with it?

Even if an organisation 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 not limited to for-profit companies.

Image by pch.vector on Freepik

Is GDPR something positive?

- GDPR is there to protect your rights as a user.
- It's good to know what you're consenting to and what cookies mean.
- Managing vulnerable customers well is not only something the law expects, but also the right thing to do socially and a smart business move.

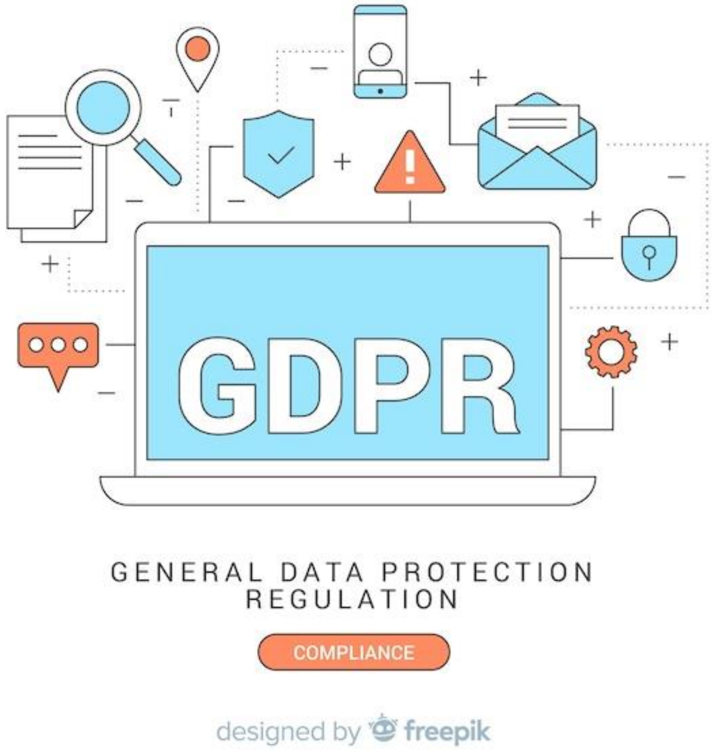


Image on Freepik

Unit 5

How you can protect yourself in advance

Objectives

On completion you will know:

✓ How you can protect yourself by identifying safe sites, links, cookies, consents

Image by vectorjuice on Freepik

Co-funded by the European Union

Some examples for you to be safe (1/3)

- 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.

Some examples for you to be safe (2/3)

- 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.

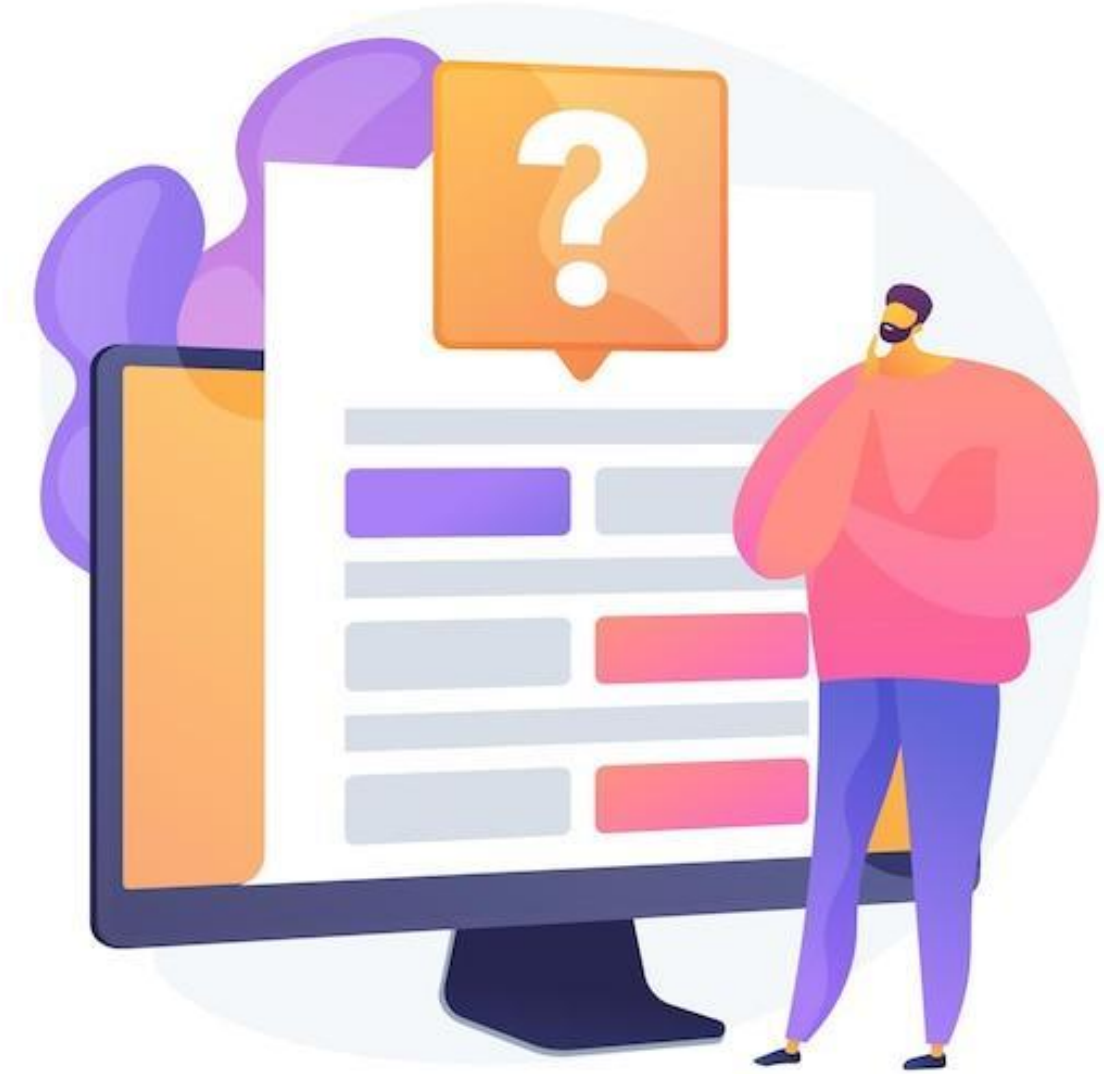
Some examples for you to be safe (3/3)

- More precautions can be taken to avoid scams.
- 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.

Check your knowledge!



Co-funded by the European Union

Image by vectorjuice on Freepik

1. Which of the following passwords is stronger?

Only one answer is correct!

A. John1234

B. John1990

C. John051190

D. J0Hn!2nO

2. Which of the following is personal data

Only one answer is correct!

A. IP address

B. E-mail address

C. All of them

D. Cookies IDs in the browser

3. When the lock symbol appears in the browser it means that the browser has locked the page because it is not secure.

Yes, the statement is correct.

No, the statement is wrong.

4. Which of the following is NOT sensitive personal data

Only one answer is correct!

A. Photos

B. Home address

C. Health related data

D. Political opinions

5. Can the sender be an indicator of whether an email is spam?

Yes

No

6. What should you never do if you receive a supposed spam-mail?

Only one answer is correct!

A. Delete the e-mail

B. Check the sender

C. Check the reference line

D. Reply and ask if it is a spam-mail

MOBILE MONEY

Congratulations!

You have completed this topic!

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Un
nor EACEA can be held responsible for them. Project number: 2023-1-RO01-KA220-ADU-000157797