



Ελενί • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



Online security for Adult Learners

Kalamata Second Chance School

Kalamata, Greece 15-19/12/2025

Eleni Lianou



Ελεni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



Day 1

Introduction to Online Security



Ελεni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



Online security





Ελεni • 3 λεπτά

Erasmus + Digiraise



Funded by the
European Union

Educational meeting 15-19 December 2025



Online scam ?



Ελεni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



Hacking Incident ?



Eleni • 3 λεπτά

Erasmus + Digiraise



Funded by the
European Union

Educational meeting 15-19 December 2025



**protection of personal
information, devices from**



Eleni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



from
digital threats like
- viruses
- hacking
- identity theft
-



Ελεni • 3 λεπτά

Erasmus + Digiraise



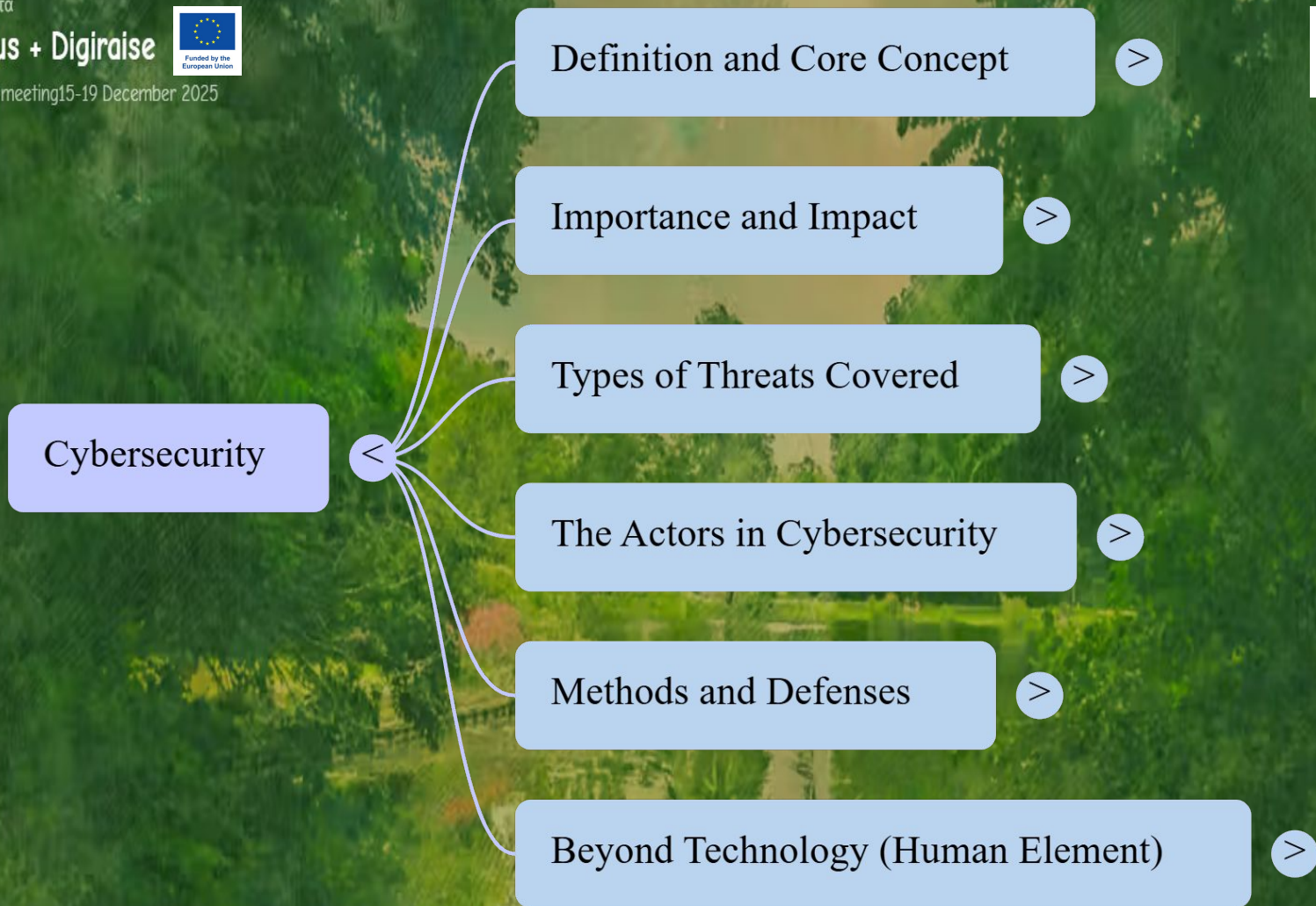
Educational meeting 15-19 December 2025



Overview of online security: What it is and why it's important.

Cybersecurity



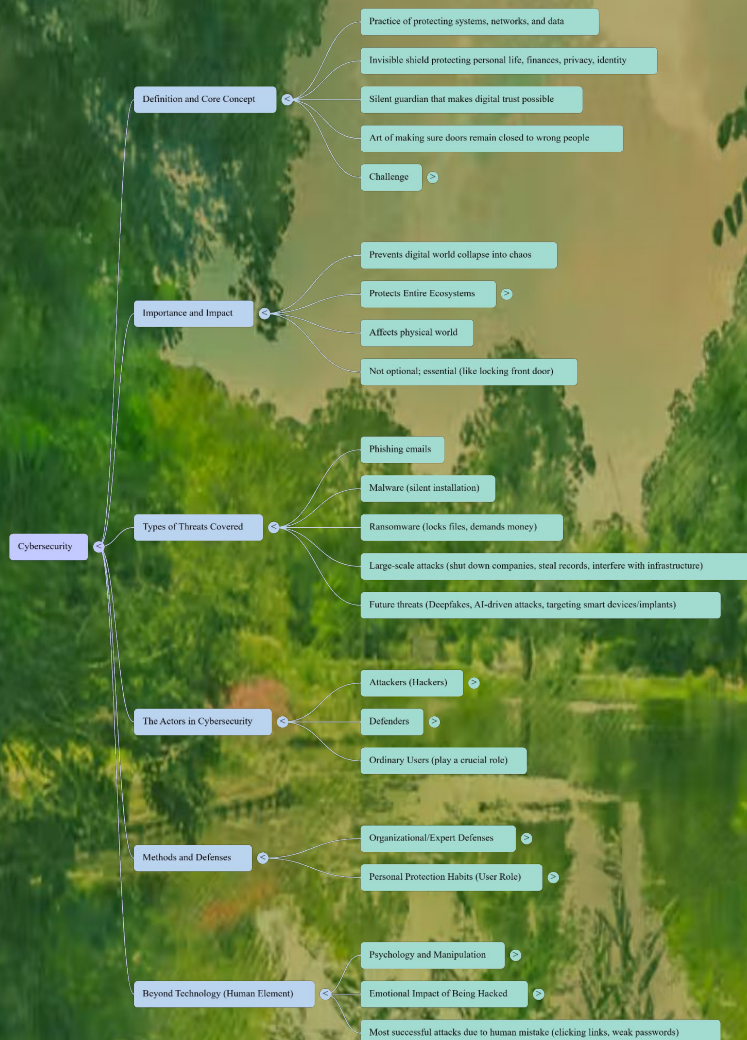




Eleni • 3 λεπτά

Erasmus + Digiraise

Educational meeting 15-19 December 2025







Eleni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



Cybersecurity is about trust



Ελεni • 3 λεπτά

Erasmus + Digiraise



Funded by the
European Union

Educational meeting 15-19 December 2025



No system is 100% sure



Ελεni • 3 λεπτά

Erasmus + Digiraise



Funded by the
European Union

Educational meeting 15-19 December 2025



Every wall has cracks



Eleni • 3 λεπτά

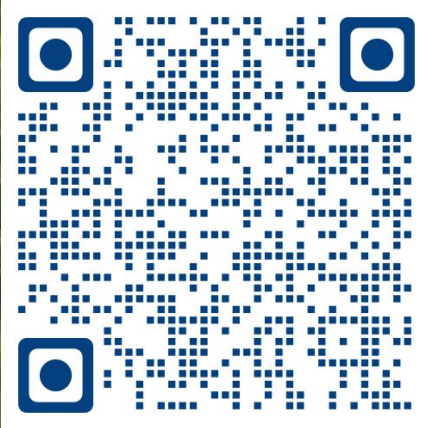
Erasmus + Digiraise



Educational meeting 15-19 December 2025



Quiz





Eleni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



Firewalls



Eleni • 3 λεπτά

Erasmus + Digiraise



Funded by the
European Union

Educational meeting 15-19 December 2025



Firewalls

a network security system, like a digital security **guard**, that monitors and controls incoming/outgoing traffic between a trusted network (your home/office) and untrusted ones (the internet) based on set rules, preventing unauthorized access and malicious data from getting in or out, acting as a vital barrier using hardware, software, or both



Eleni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025

**Attackers
only need
to succeed
once**

while defenders
need to
succeed

EVERY

SINGLE TIME



Ελεni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



White hat hackers

hackers

Cybersecurity professionals



Ελεni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



Cybersecurity is about psychology



Eleni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



Hackers attack the humans that use the machines



Eleni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



Cybersecurity gives you Control



Ελεni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



– *Common threats: Phishing*

What is Phishing?

Don't Take the Bait: A Guide to Phishing Attacks

THE THREAT: HOW PHISHING HOOKS ITS VICTIMS

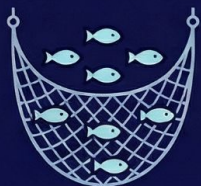
What is a Phishing Attack?

A fraudulent message designed to trick you into revealing sensitive personal information.



counterfeit website

Common Types of Phishing



Deceptive Phishing

Thousands of random users
A general, non-personalized fraudulent email.



Spear Phishing

A specific individual or group
A customized message using researched information.



Whaling

High-value individuals
(e.g., CEOs)
A highly-researched, meticulously planned attack.

THE SOLUTION: HOW TO STAY OFF THE HOOK



Always Verify Links

Check that the link goes to a secure (HTTPS) and authentic website address.



Scrutinize Suspicious Messages

Do not enter private data on pop-up windows or from unsolicited emails.



Use Anti-Phishing Tools

Install secure browser extensions designed to identify and block malicious emails.



Ελεni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



Fake message

often called a **scam** or **phishing** text (**smishing**), is a deceptive message designed to trick you into revealing personal info (passwords, bank details, SSN), sending money, or downloading malware, usually by impersonating trusted entities like banks or delivery services, creating false urgency, and including malicious links or urgent requests for personal data.



Ελεni • 3 λεπτά

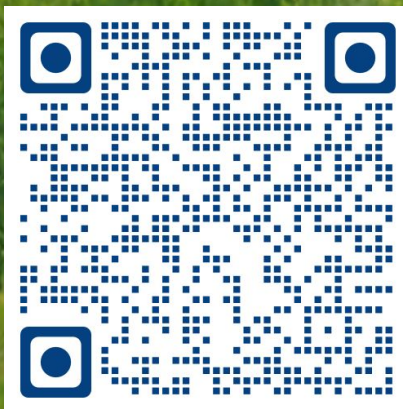
Erasmus + Digiraise



Educational meeting 15-19 December 2025



Quiz





Ελεni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



Smishing

(SMS + phishing) tricks you into giving up personal info via text message, pretending to be a trusted source like a bank or delivery service to create urgency (e.g., "Your account is locked!"). Scammers use malicious links to steal data or install malware, leveraging the personal, immediate nature of texts to get you to click without thinking, leading to identity theft or financial fraud.



Eleni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025

Spearfishing

a highly targeted phishing attack focused on high-profile individuals like C-suite executives (CEOs, CFOs) or other senior leaders, tricking them into revealing sensitive data, authorizing fraudulent transactions (like wire transfers), or granting system access, often by impersonating trusted sources to exploit their authority and bypass security. These attacks are sophisticated, personalized, and aim for significant financial gain or major data breaches, differing from general phishing by focusing on "big fish" (whales) with high-value access





Eleni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025

Whaling



a highly targeted phishing attack focused on high-profile individuals (CEOs, CFOs) tricking them into revealing sensitive data, authorizing fraudulent transactions, or granting system access, to exploit their authority and bypass security. These attacks are sophisticated, personalized, and aim for significant financial gain or major data breaches, differing from general phishing by focusing on "big fish" (whales) with high-value access



Ελεni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



Pharming

ARP Spoofing
DNS cache poisoning

is a type of online fraud that directs victims to spoofed websites in an attempt to steal their credentials and data.

www.facebook.com

www.facebok.com



Eleni • 3 λεπτά

Erasmus + Digiraise



Funded by the
European Union

Educational meeting 15-19 December 2025



ARP Spoofing

Address Resolution Protocol

tricks devices on a local network (LAN) into sending traffic to an attacker by faking IP-to-MAC address links, enabling man-in-the-middle (MitM) interception.



DNS cache poisoning

Domain Name System

is a cyberattack that injects false IP address information into a DNS resolver's cache, tricking it into redirecting users from legitimate websites to malicious ones, often to steal credentials or install malware.



Eleni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



– ***Common threats: malware***

Hacker Explains Malware





GPU: allows to perform simple tasks simultaneously through parallel processing, making it ideal for 3D graphics rendering, video editing, machine learning.



***Graphics Processing Unit, is
a specialized electronic
circuit that rapidly handles
visual and mathematical
calculations to create images
for a screen.***



***GPUs can be found as
dedicated cards or
integrated directly into a
computer's main processor
(CPU).***

A botnet is a network of internet-connected devices (computers, IoT gadgets, etc.) infected with malicious software, allowing a cybercriminal (bot-herder) to control them remotely as "bots" or "zombies" to launch large-scale attacks like DDoS, send spam, steal data, or mine cryptocurrency, often without the owners' knowledge.

ANATOMY OF A BOTNET ATTACK



THE HACKER'S PLAYBOOK: A 4-STEP ATTACK



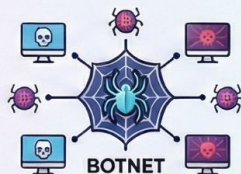
1. Identify a Target

The hacker targets engineering students, knowing they own powerful computers with good GPUs.



2. Select the Malware

A botnet is chosen to secretly control multiple infected computers for a single purpose.



3. Craft the Delivery

The botnet code is hidden in a PDF disguised as a free textbook.

4. Launch the Attack

The PDF is sent from fake professor email accounts to trick students into downloading it.



YOUR 3-STEP DEFENSE PLAN



Use Protection Software

Malware protection can automatically scan, detect, and remove known threats from your device.



Keep Devices Updated

Regular updates patch known vulnerabilities that hackers can exploit to gain access.



Don't Trust Unsolicited Files

Avoid downloading and running files, especially from unknown or suspicious sources.





These devices communicate via command-and-control (C&C) servers, enabling coordinated, powerful attacks by leveraging the combined computing power of the infected machines



Eleni • 3 λεπτά

Erasmus + Digiraise



Funded by the
European Union

Educational meeting 15-19 December 2025



– ***Common threats: Entity theft***



Eleni • 3 λεπτά

Erasmus + Digiraise



Funded by the
European Union

Educational meeting 15-19 December 2025



IDENTITY THEFT

Protecting Yourself From Identity Theft

HOW FRAUDSTERS STEAL YOUR IDENTITY



Physical Theft

Stealing mail, dumpster diving, or taking discarded devices with unwiped hard drives.

Social Engineering

Tricking you into giving up info via phishing or impersonating trusted entities.



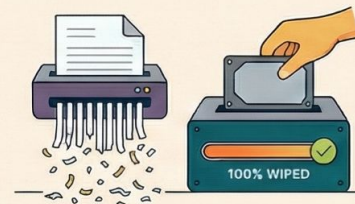
High-Tech Attacks

Using malware or hacking large organizations to steal data from many people at once.

YOUR DEFENSE & RESPONSE PLAN

Secure Physical & Digital Data

Shred sensitive documents and wipe all hard drives before disposal.



Be Vigilant Online & On Calls

Avoid unsecured public Wi-Fi and verify requests for personal information.

If You Become a Victim...



Immediately freeze financial accounts, check credit reports, and file official reports.



Ελεni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



– ***Common threats: ransomware***



What is Ransomware?

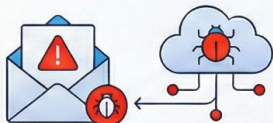
This infographic provides a high-level overview of ransomware attacks, identifying key components and consequences. These attacks can affect computer systems and files, with financial demands as a central component.

THE ATTACK

Ransomware is a type of attack on computer systems.



It can impact documents, files, and entire networks.



Attacks can spread through email.

Malicious emails are a common way for systems to get infected.



Critical sectors like hospitals are targeted.

These attacks can disrupt essential services for the public.

THE RANSOM

Attackers demand money to restore access.

This is the central component of a ransomware attack.



Paying the ransom does not guarantee recovery.

There is no certainty that files will be returned after payment.



– *Common threats: ransomware*

a cyberattack where malicious software (malware) encrypts a victim's files or locks their device, preventing access until a ransom (usually in cryptocurrency) is paid for decryption, often delivered via phishing emails, malicious links, or infected downloads, and sometimes involves stealing and threatening to leak data (double extortion).



Eleni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



Locker ransomware

a type of malware that completely blocks a user's access to their computer system or device, typically leaves the files themselves untouched but makes the entire system inoperable by displaying a full-screen ransom note or changing critical system settings like the PIN or password



Eleni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025

Crypto ransomware

the attacker encrypts a  victim's sensitive data or files so that they can't access them unless they pay a requested ransom. In theory, once the victim pays, the attacker turns over a decryption key that gives them access to the files or data, however, there's no guarantee



Scareware

locks users out of their devices or encrypts critical files, making the system unusable until a ransom is paid. The main purpose of ransomware is extortion, as it requires the payment of money, mostly in cryptocurrency for the restoration of access to the compromised data system.





Ελεni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



***– Real-life examples of
security breaches and
their impacts.***



Eleni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



5 REAL-LIFE CYBER ATTACKS

HOPLON
INFOSEC



Eleni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



Principles of strong passwords.

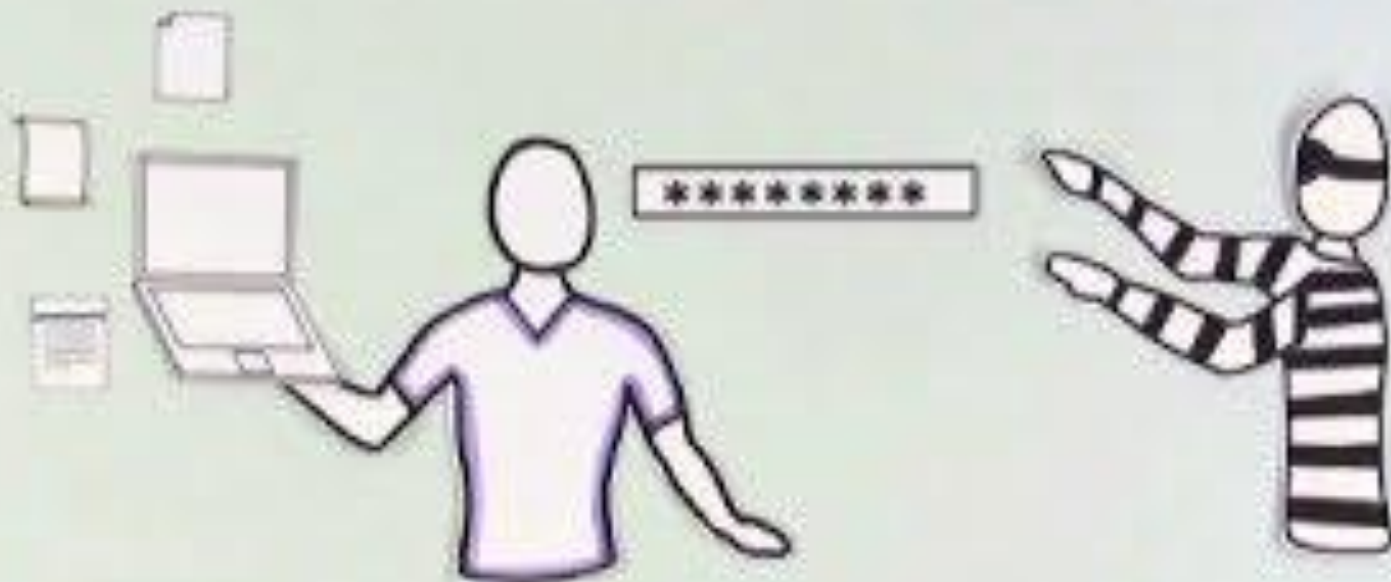


Eleni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025





Eleni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



– *How to use password managers*



How to Create and Protect a Strong Password

Avoid Using Personal Information

Don't use pet names, birth dates, or addresses that criminals can easily discover.



Use a "Passphrase" Acronym

*Jack and Jill
went up
the hill*

JaJwutH

Turn a memorable phrase like "Jack and Jill went up the hill" into "JaJwutH".



STRONG PASSWORD

Add Complexity

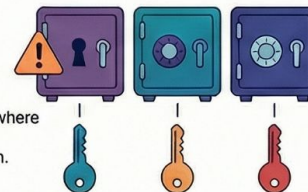


Make your password even stronger by adding uppercase letters, numbers, and special characters.

PROTECT YOUR PASSWORD

Don't Reuse the Same Password

Using one password everywhere is like having one key that unlocks everything you own.



Keep It a Secret

Never share your password over the phone or email, as it could be a scam.

Log Out on Public Computers

Always log out of websites to prevent the next user from accessing your accounts.





Ελεni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



– Setting up two-factor authentication (2FA)





Ελεni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



Quiz



Ελεni • 3 λεπτά

Erasmus + Digiraise



Educational meeting 15-19 December 2025



Quiz 3



Eleni • 3 λεπτά

Erasmus + Digiraise



Funded by the
European Union

Educational meeting 15-19 December 2025



Thank you!!