Co-funded by the European Union

LESSON 11

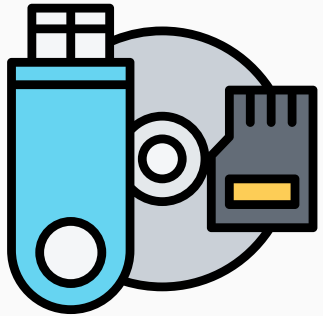
DATA AND DEVICE PROTECTION

I.MAM VIRTUAL – 101083431 Programme(s): Erasmus+ (ERASMUS+) Topic(s): ERASMUS-EDU-2021-VIRT-EXCH-NDICI Type of action: ERASMUS Project Grants ERASMUS-EDU-2021-VIRT-EXCH- Virtual Exchanges

Co-funded by
the European Union

Data and Device Protection

Data and device protection is a critical aspect of modern information security. With the increasing reliance on digital devices and the vast amounts of data generated daily, ensuring the safety and privacy of both data and devices has become paramount. This presentation will cover key concepts, threats, and strategies for effective data and device protection.



Co-funded by
the European Union

Data Protection

Definition: Safeguarding personal and sensitive data from unauthorized access, corruption, or theft.
Importance: Protects privacy, maintains trust, and ensures compliance with regulations like GDPR and CCPA.

Device Protection

Definition: Ensuring the security of physical and virtual devices from threats that can compromise their integrity.
Importance: Prevents unauthorized access, protects against malware, and ensures the proper functioning of devices.

Co-funded by
the European Union

Common Threats

Co-funded by
the European Union

Data Threats

Data Breaches: Unauthorized access to sensitive data.
Data Corruption: Accidental or intentional alteration of data.
Data Loss: Permanent loss of data due to hardware failure, human error, or cyberattacks.

Device Threats

Malware: Malicious software designed to disrupt, damage, or gain unauthorized access to devices.
Phishing: Fraudulent attempts to obtain sensitive information by disguising as a trustworthy entity.
Physical Theft: Loss or theft of devices leading to potential data breaches.

Co-funded by
the European Union

Strategies for Data Protection

Co-funded by
the European Union

Encryption

Definition: Converting data into a code to prevent unauthorized access.
Application: Use strong encryption for data at rest and in transit.

Access Controls

Definition: Mechanisms that limit access to data based on user roles.
Application: Implement multi-factor authentication (MFA) and least privilege access principles.

Regular Backups

Definition: Creating copies of data to restore in case of data loss.
Application: Schedule regular backups and store them in secure, off-site locations.

Co-funded by
the European Union

Strategies for Device Protection

Co-funded by
the European Union

Antivirus and Anti-Malware Software

Definition: Programs designed to detect and remove malicious software.
Application: Install reputable antivirus software and keep it updated.

Secure Configurations

Definition: Setting up devices with security best practices in mind.
Application: Disable unnecessary services and applications, change default passwords, and apply security patches.

Physical Security Measures

Definition: Protecting devices from physical threats.
Application: Use locks, secure storage, and track devices to prevent theft or unauthorized access.

Co-funded by
the European Union

Emerging Technologies in Protection

Co-funded by
the European Union

AI and Machine Learning

Application: Detect and respond to threats in real-time using predictive analytics.

Blockchain

Application: Ensure data integrity and enhance secure transactions with decentralized ledger technology.

Co-funded by
the European Union

THANK YOU!

“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.”