Co-funded by
the European Union

Course: IT Fundamentals of Cyber Security

Project: Cyber Security 4 ALL(CS4ALL)

CHAPTER I

Introduction to Information Technology and Cyber Security

Content

- ✓ Overview of IT fundamentals
    - ✓ Essential components of Information Technology
    - ✓ Core Components of IT Infrastructure and IT System Architecture
    - ✓ Challenges and Future trends in IT
- ✓ Importance of cybersecurity in modern IT environments
    - ✓ Importance in Protecting data and system
    - ✓ Growing prevalence of Cyber threats
    - ✓ Role in Ensuring Policy and confidentiality
- ✓ Basic concepts and terminology in cybersecurity
    - ✓ Cyber Security Concepts
    - ✓ Importance of protecting digital information
    - ✓ Cyber Security Threats , Measures and Terminology

Co-funded by
the European Union

Co-funded by
the European Union

Overview of IT fundamentals

✓ **Definition of Cybersecurity:**

Cybersecurity encompasses any technology, measure, or practice aimed at preventing or mitigating cyber threats.

✓ **Purpose of Cybersecurity:**

The primary goal of cybersecurity is to protect individuals' and organizations' systems, applications, and computing devices.

✓ **Protection of Sensitive Data:**

Cybersecurity safeguards sensitive data and financial assets against threats such as computer viruses and sophisticated attacks.

Co-funded by
the European Union

Essential components of Information Technology

People: The most important part as they make end users more productive

Procedure: Refer to rules or guidelines people follow when using software, hardware, and data

Software: It is the term for programs or sets of computer instructions written in a special computer language that enables a computer to accomplish a given task

Hardware: Refers to physical, touchable pieces or equipment.

Data: Raw, unprocessed facts including text, numbers, images and sounds

CS4ALL
CYBERSECURITY FOR ALL

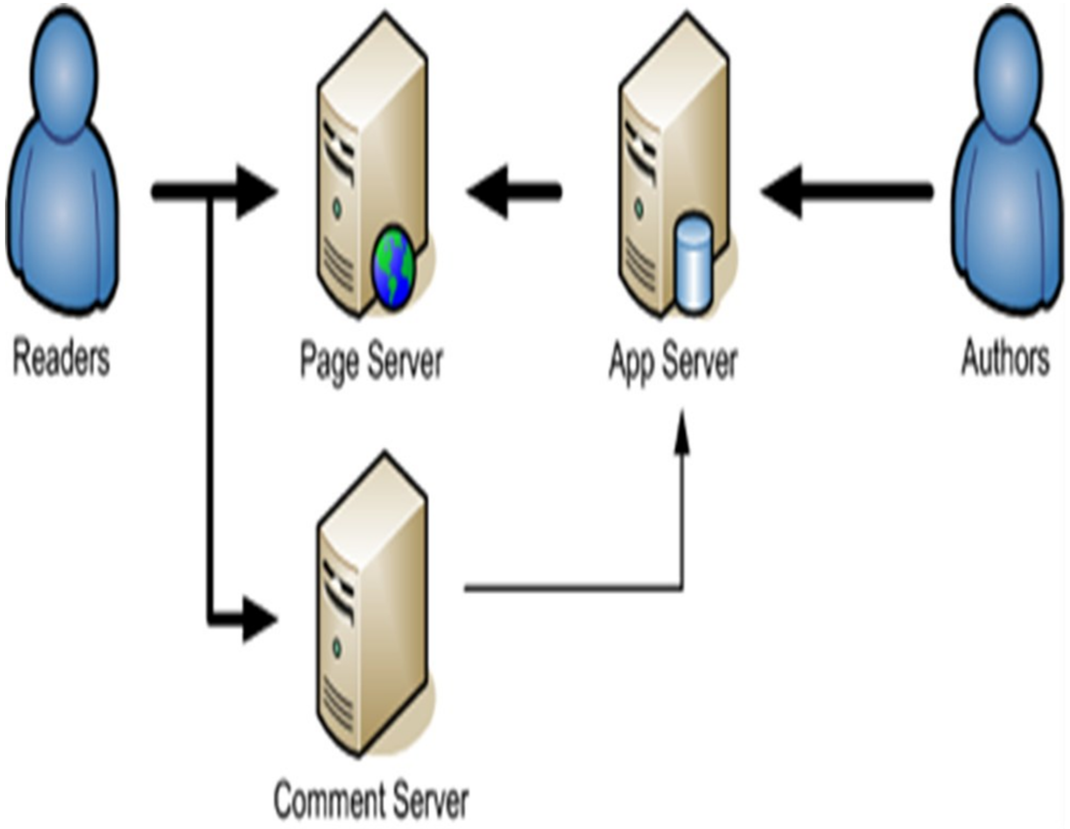
IT Infrastructure and Architecture

Core Components of IT Infrastructure and IT System Architecture

Hardware:
Includes personal computers, servers, routers, and other physical devices essential for IT operations.

Software:
Comprises applications used by an organization, web servers, and operating systems that facilitate business functions.

Networking:
Ensures smooth network operations and communication between different IT components.



Co-funded by the European Union

Challenges in Information Technology

- **Workload**

  Managing Increasing Workloads is a key challenge in IT

- **Cyber Security**

  Ensuring robust cyber security measures is critical to protect data and system

- **Skills Gap**

  There is s Notable gap in necessary skills among IT Professionals

- **Digital Transformation**

  Organizations face challenges in effectively implementing digital transformation strategies

- **Cloud Computing**

  Navigating the Complexities of cloud computing can be challenging for IT teams

Co-funded by
the European Union

Challenges in Information Technology

- **Hiring**

  Recruiting the right talent remains a significant obstacle in the IT landscape.

- **Budget**

  Limited budgets often hinder the ability to address various IT challenges.

- **Leadership Support in prioritizing New Skill Development**

  Effective leadership support is essential for prioritizing new skills development within teams.

- **Analytics and Data Management**

  Managing and analyzing data effectively poses a challenge for many organizations.

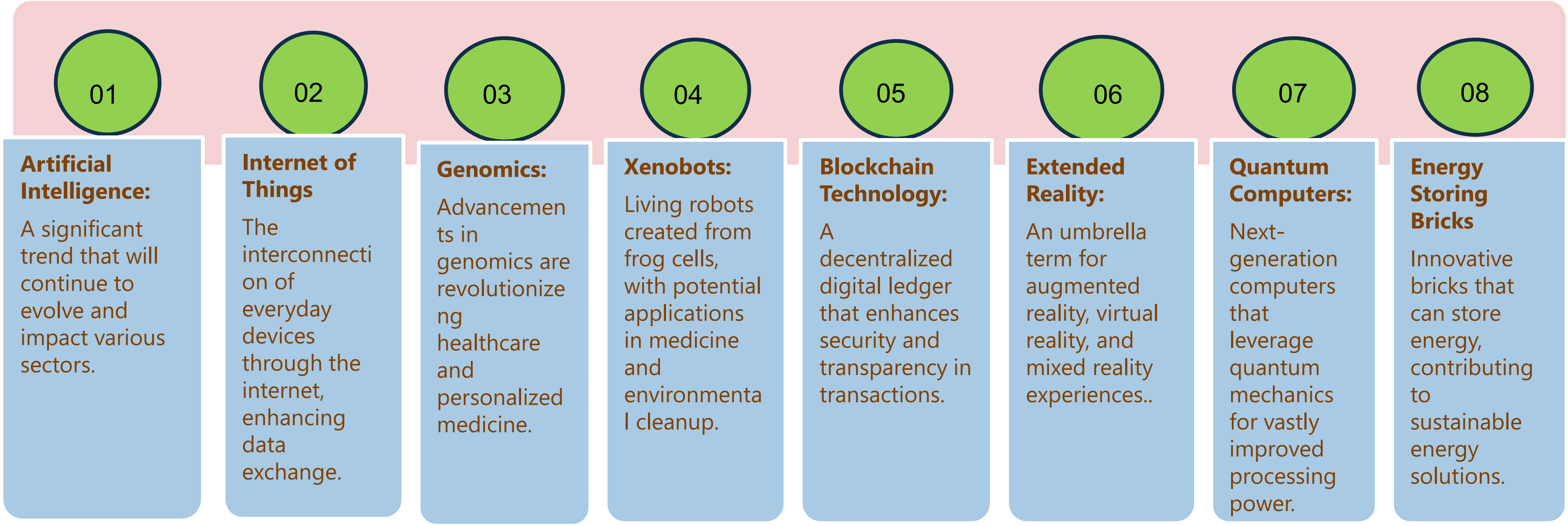
- **Automation**

  Integrating automation tools and processes can be complex and requires careful planning

Co-funded by
the European Union

Future Trends in IT

Top Eight Future Technology Trends



01

Artificial Intelligence:

A significant trend that will continue to evolve and impact various sectors.

02

Internet of Things

The interconnection of everyday devices through the internet, enhancing data exchange.

03

Genomics:

Advancements in genomics are revolutionizing healthcare and personalized medicine.

04

Xenobots:

Living robots created from frog cells, with potential applications in medicine and environmental cleanup.

05

Blockchain Technology:

A decentralized digital ledger that enhances security and transparency in transactions.

06

Extended Reality:

An umbrella term for augmented reality, virtual reality, and mixed reality experiences..

07

Quantum Computers:

Next-generation computers that leverage quantum mechanics for vastly improved processing power.

08

Energy Storing Bricks

Innovative bricks that can store energy, contributing to sustainable energy solutions.

Co-funded by
the European Union

Importance of Cybersecurity

Importance of Cybersecurity in Modern IT Environment

01

Data Protection

Data protection is the process of safeguarding data from corruption, loss, or unauthorized access, making it an essential practice in cybersecurity.

02

Data Assets

All forms of data are considered valuable assets for an organization or institution, highlighting the need for robust cybersecurity measures.

Co-funded by
the European Union

Data Protection Significance

01 Fundamental Right

Data protection is a fundamental right that is safeguarded by law.

02 Builds Trust

Effective data protection measures help to establish and build trust with customers.

03 Branding

Incorporating data protection into your branding strategy enhances your organization's reputation.

04 Prevention of Fraud

Data protection plays a crucial role in preventing fraud and cybercrimes.

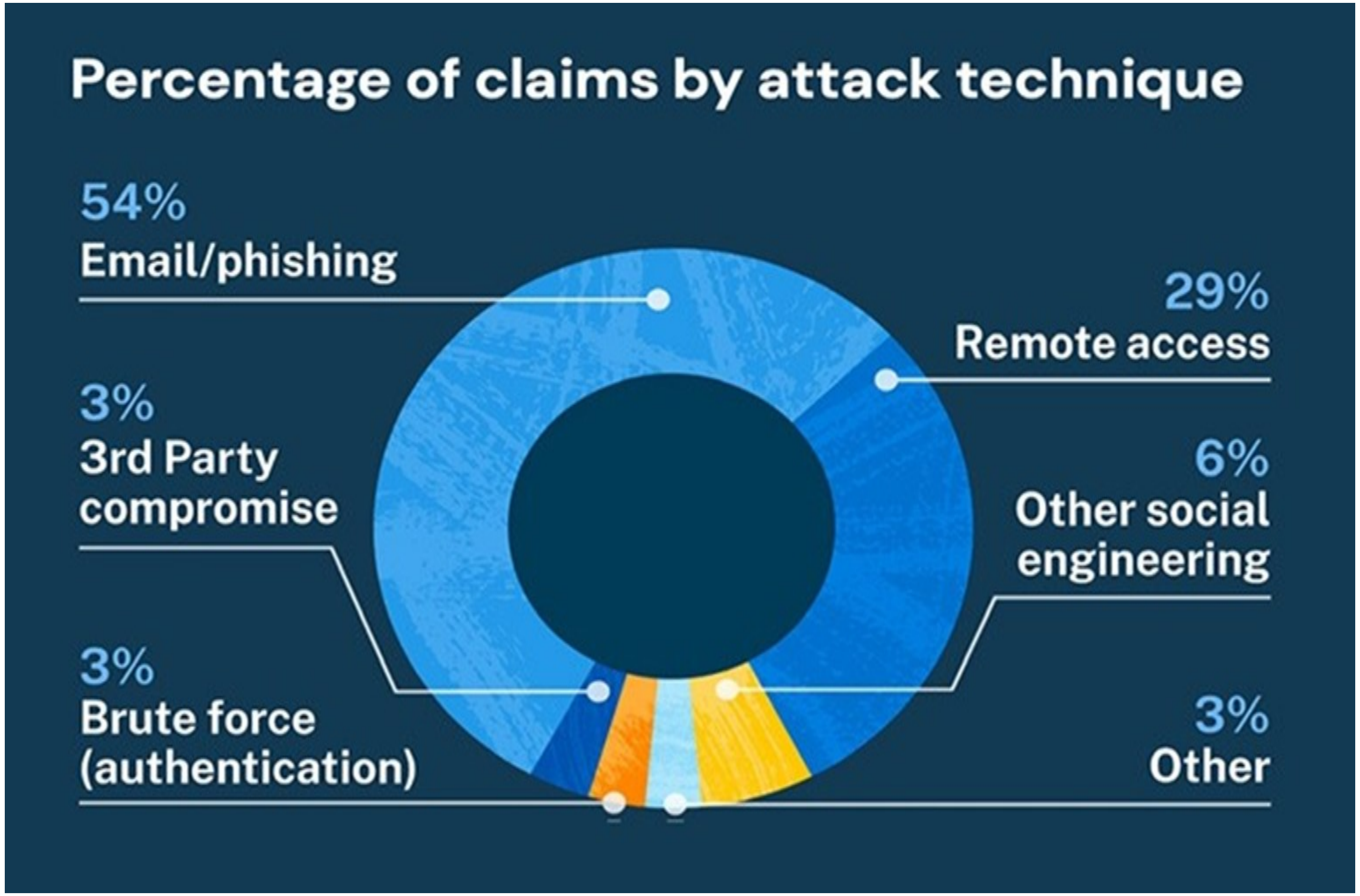
05 Cost-Effective

Implementing data protection can save organizations time and money in the long run.

CS4ALL CYBERSECURITY FOR ALL

Co-funded by
the European Union

Growing prevalence of Cyber Threats



Co-funded by
the European Union

Role in Ensuring Policy and confidentiality

Ensuring Security and Confidentiality in IT Systems

Security Policy:

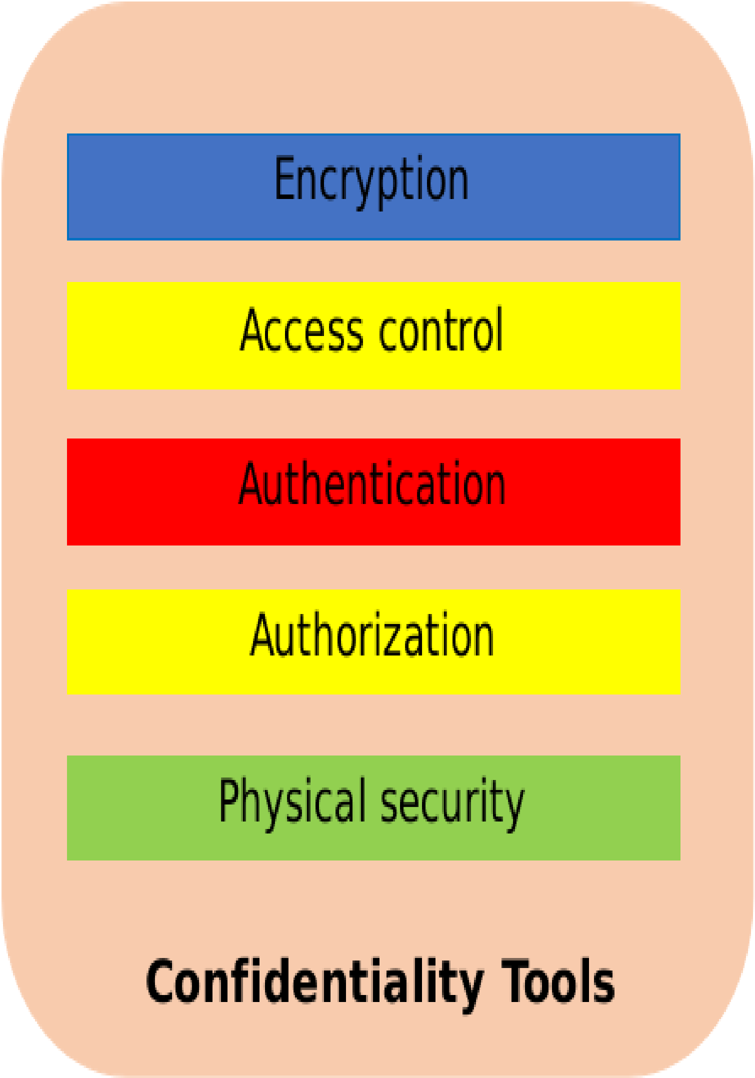
A security policy is a statement designed to guide employees' behavior regarding the security of company information and IT systems.

Confidentiality:

Confidentiality is a core component of security policies, ensuring that sensitive information is protected from unauthorized access.

Tools for Confidentiality:

Various tools and practices are implemented to maintain confidentiality and safeguard company data.


Encryption

Access control

Authentication

Authorization

Physical security

Confidentiality Tools

Co-funded by
the European Union

Tools for Confidentiality

01 **Encryption:** Utilizing cryptographic methods to protect data confidentiality.

02 **Access Control:** Implementing measures to restrict access to sensitive information.

03 **Authentication:** Verifying the identity of users before granting access to systems.

04 **Authorization:** Determining what resources a user can access after authentication.

05 **Physical Security:** Protecting physical assets and locations from unauthorized access.

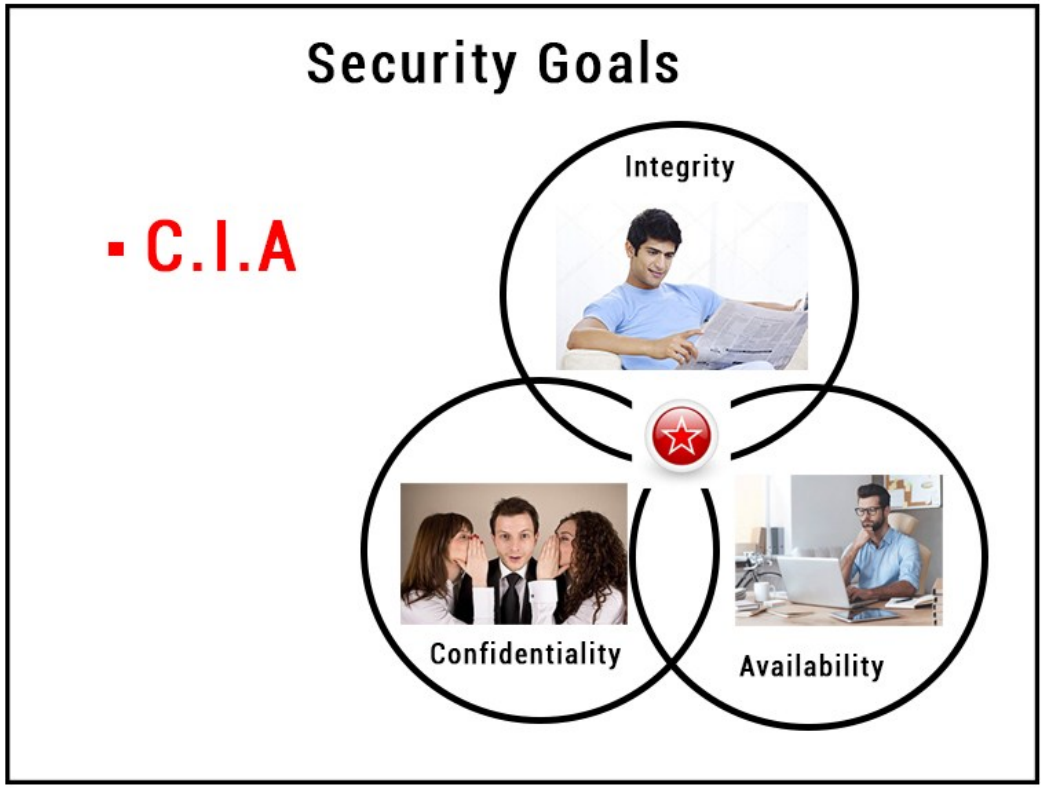
06 **Integrity:** Ensuring the accuracy and reliability of data throughout its lifecycle.

Co-funded by
the European Union

Cyber Security Goals

Cybersecurity can be measured by at least one of three goals-

- **Protect the confidentiality of data.**
- **Preserve the integrity of data.**
- **Promote the availability of data for authorized users.**



Security Goals

- C.I.A

Co-funded by
the European Union

Basic Cybersecurity Concepts

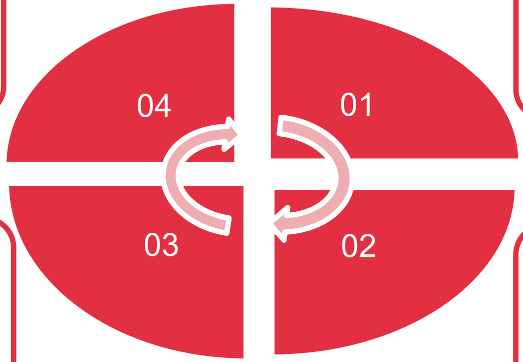
Basic concepts and terminology in cybersecurity

- Abuse

  The improper use of a system or resource that can lead to harm or damage.

- Threat

  A potential cause of an unwanted incident that may result in harm to a system or organization.



- Attack

  An intentional act that aims to cause damage or disruption to as System or network.

- Vulnerability

  A weakness in a system that can be exploited by threats to gain unauthorized access or cause harm.

Co-funded by
the European Union

Protecting Digital Information

Importance of protecting Digital Information

Data Protection For businesses

◆ Trust and Reputation

◆ Legal and Financial Consequences

◆ Intellectual Property Protection

◆ Competitive Advantage

Data Protection for Individuals

◆ Personal Privacy

◆ Avoiding Financial Loss

◆ Identity Protection

◆ Protection from Cyberbullying

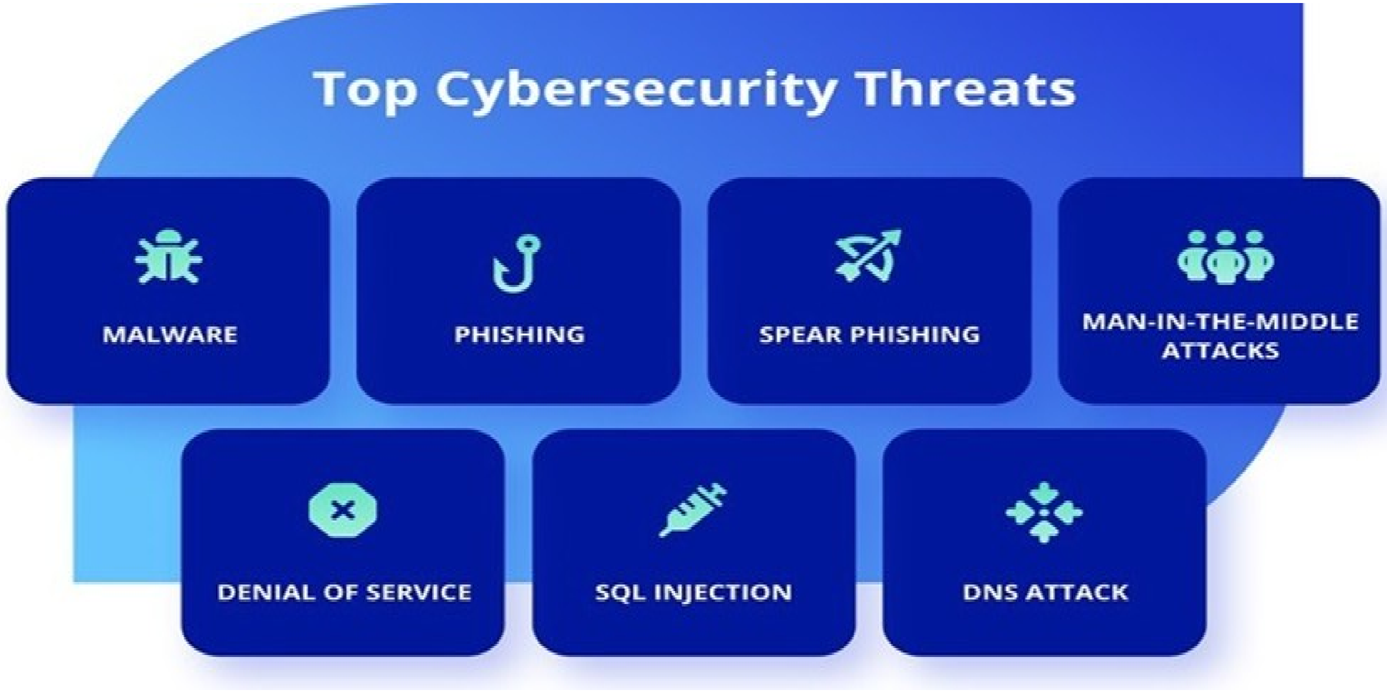
◆ Preserving Digital Legacy

Co-funded by
the European Union

Cybersecurity Threats, Measures and Terminology

Threat

A threat is any incident that could negatively affect an asset – for example, if it’s lost, knocked offline or accessed by an unauthorized party.



Co-funded by
the European Union

Malware

Malware is a software that is designed to attack, control and damage a device’s security and infrastructure systems

Types of Malware

- ❑ **Ransomware** : A type of malware that prevents or limits users from accessing their system
- ❑ **Fileless Malware** : Malicious code that works directly within a computer's memory instead of the hard drive
- ❑ **Mobile Malware** : Malicious software specifically designed to target mobile devices
- ❑ **Wiper Malware** : Deletes or destroys an organization's access to files and data.
- ❑ **Hybrid Malware** : Combination of two or more different types of attacks
- ❑ **Cryptojacking** : Type of cybercrime that involves the unauthorized use of people's devices

Co-funded by
the European Union

MITM and Real-life Instances

Definition of MITM Attack

A man-in-the-middle (MITM) attack is a form of cyber-attack where a malicious individual introduces themselves into a meeting between two parties.

Nature of MITM Attacks

MITM attacks can involve various methods to intercept or alter communications between the involved parties without their knowledge.

Real-life Instances of MITM Attacks

There are numerous real-world examples demonstrating the impact and execution of MITM attacks, highlighting the importance of cybersecurity awareness.

CS4ALL CYBERSECURITY FOR ALL

Co-funded by the European Union

Denial of Service and SQL Injection

01

Denial of Service (DoS)
DoS is a cyber-attack that targets an individual computer or website, aiming to make it unavailable to users.

02

Impact of DoS Attacks
These attacks can disrupt services, leading to significant downtime and potential financial losses.

03

SQL Injection
SQL injection is a code injection technique used by attackers to manipulate databases by inserting malicious SQL statements.

04

Consequences of SQL Injection
Successful SQL injection attacks can lead to unauthorized access to sensitive data and compromise the integrity of a database.

Co-funded by
the European Union

Cybersecurity Terminology

- **Authentication :** Verification, validation, evidence, proof, identification, documentation
- **Botnet :** Network of infected computers
- **Data Breach :** Data leak or data spill
- **DDoS :** Cybercrime in which the attacker floods a server with internet
- **Domain :** Field of influence, thought, or action
- **Encryption :** The process of converting data into a code to protect it
- **Exploit :** A piece of code or program that takes advantage of a security vulnerability
- **Firewall :** A network security system that prevents unauthorized access to a computer network.

CS4ALL
CYBERSECURITY FOR ALL
Co-funded by
the European Union

Cybersecurity Terminology

- **Hacker, Black Hat :** A computer hacker who violates laws
- **Hacker, White Hat :** Ethical hackers or good hackers
- **Malware :** Malicious software
- **Man in the Middle Attack :** Cyberattack where the attacker secretly relays
- **Phishing** : Involves tricking people into sharing sensitive information
- **Ransomware :** A type of malware that locks a victim's device
- **Spoofing :** A type of scam where a criminal pretends gain the trust of a victim.
- **Spyware :** Malicious software that collects information from system without your consent

Co-funded by
the European Union

Resources

List the resources used for research:

1. Chwan-Hwa (John) Wu, J. David Irwin, Introduction to Computer Networks and Cyber security, CRC Press T&F Group, 2013.

2. Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley

3. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press.

Co-funded by
the European Union

Questions & answers

Co-funded by
the European Union

Conclusion

In conclusion, **Information Technology (IT)** manages and supports digital systems, while **Cyber Security** protects them from threats. As digital reliance grows, safeguarding IT systems is crucial to ensure data integrity, privacy, and system functionality. The future of IT depends on strong Cyber Security practices to maintain safe and reliable digital environments.

Co-funded by
the European Union

THANK YOU