Co-funded by
the European Union

Course: IT Fundamentals of Cyber Security

Project: Cyber Security 4 ALL(CS4ALL)

CHAPTER IV

Cyber Security Threats and Vulnerability

Contents

- ✓ Types of Malwares (Viruses, worms, ransomware)
  - Importance of Understanding different types of malware
  - Overview of malwares and Impact on System and Data
- ✓ Social Engineering Techniques
  - Definition and Importance of understanding social Engineering
  - Overview and its impact on individual and Organizations
- ✓ Web Based Threats and vulnerabilities
  - Common web Based Threats
  - Web Application security Best Practices

References

Links

Co-funded by the European Union

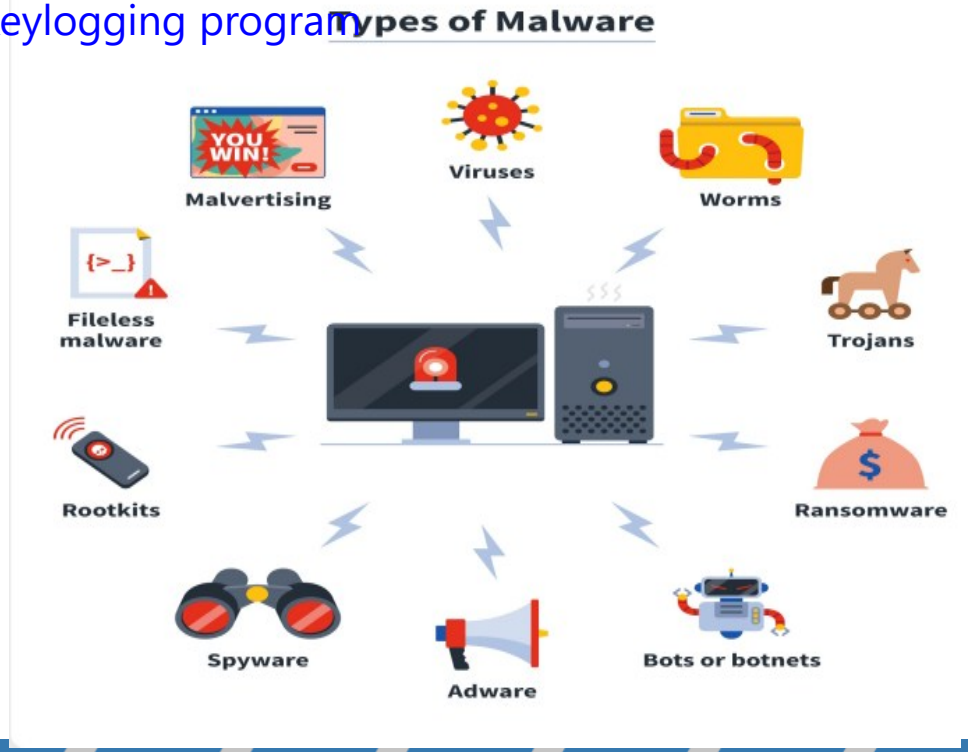
Malware

- Malware is short for malicious software and refers to any software that is designed to cause harm to computer systems, networks, or users.
- It’s important for individuals and organizations to be aware of the different types of malware and take steps to protect their systems

CS4ALL
CYBERSECURITY FOR ALL
Co-funded by
the European Union

Types of Malwares

- **Worms-**After a worm infects a host, it is able to spread very quickly over the network.
- **Trojan horse** – A Trojan horse is malware that carries out malicious operations under the appearance of desired operation such as playing an online game.
- **Ransomware** – Ransomware grasps a computer system or the data it contains until the victim makes payment
- **Adware** – It displays unwanted ads and pop-ups on the computer.
- **Spyware** – Its purpose is to steal private information from a computer system for a third party.
- **Logic Bombs** – A logic bomb is a malicious program that uses a trigger to activate the malicious code
- **Rootkits** – A rootkit modifies the OS to make a backdoor
- **Backdoors** – A backdoor bypasses the usual authentication used to access a system
- **Keyloggers**-Obtain passwords and other sensitive information and send them to the source of the keylogging program

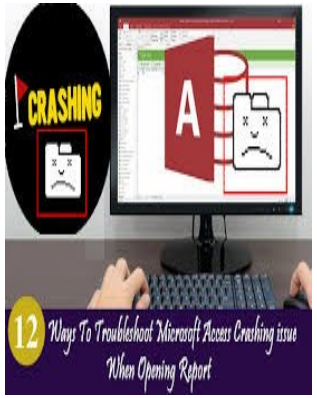


Co-funded by the European Union

Malwares Impact On System and Data

How Malware Affects Systems?

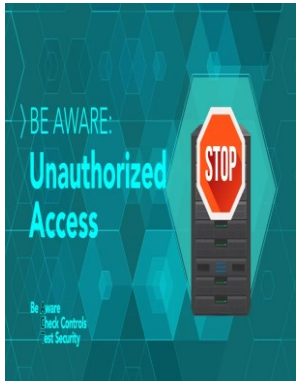
Decreased speed.



Crashing of programs.

Data corruption.

Even total system failure.



Unauthorized access

Co-funded by the European Union

To avoid getting a virus or malware

Prevention Measures

- Installing an antivirus program
- Avoiding opening suspicious links or email attachments
- Using a firewall, backing up all of your important files and data regularly
- Educating yourself about cybersecurity risks
- Using secure passwords for all accounts

Co-funded by
the European Union

Social Engineering Techniques

Co-funded by the European Union

- Definition: Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.
- Attackers trick users into breaking normal security practices.
- Techniques:
  - Phishing (e.g., fake emails).
  - Baiting (e.g., USB drives with malware).
  - Pretexting (Impersonating someone

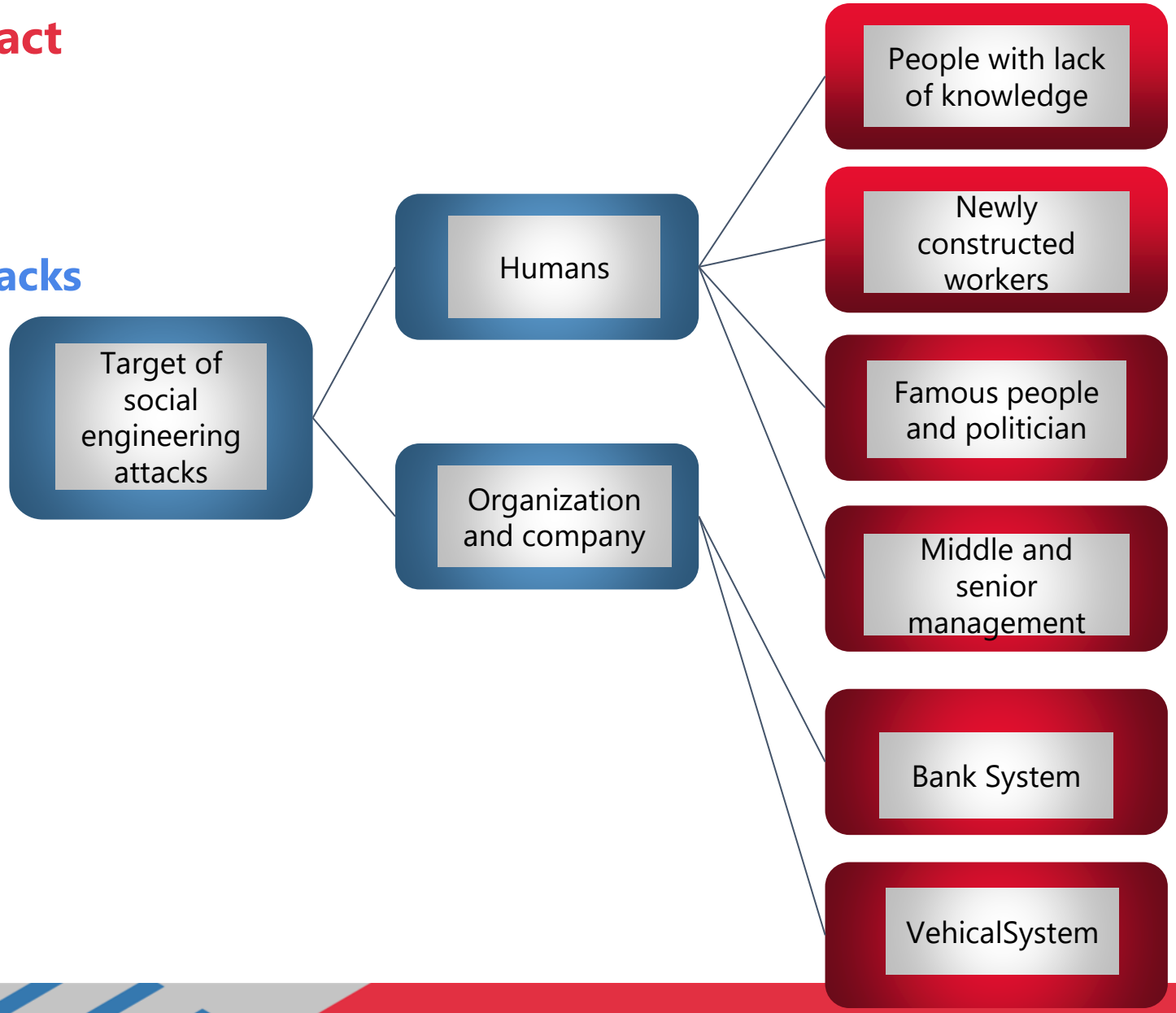
Organizational and Individual Impact

Impact on Organization

- Impact on Reputation
- Getting Hit by Ransomware
- Falling Prey to Watering Hole Attacks
- Cost on Business Productivity
- Financial Losses
- Disruption in Operations

Impact on Individual

- Identity theft
- Malware attacks
- Ransomware attacks
- Reputational damage
- Data theft
- Service disruption



Co-funded by the European Union

Preventing Social Engineering Attacks

- **Employee Training**: Create awareness of social engineering tactics.
- **Cybersecurity Tools:** Use up-to-date software to detect threats.
- **Caution:** Be wary of unsolicited emails or requests for sensitive data.
- **Regular Audits:** Review and update security protocols frequently.

Co-funded by the European Union

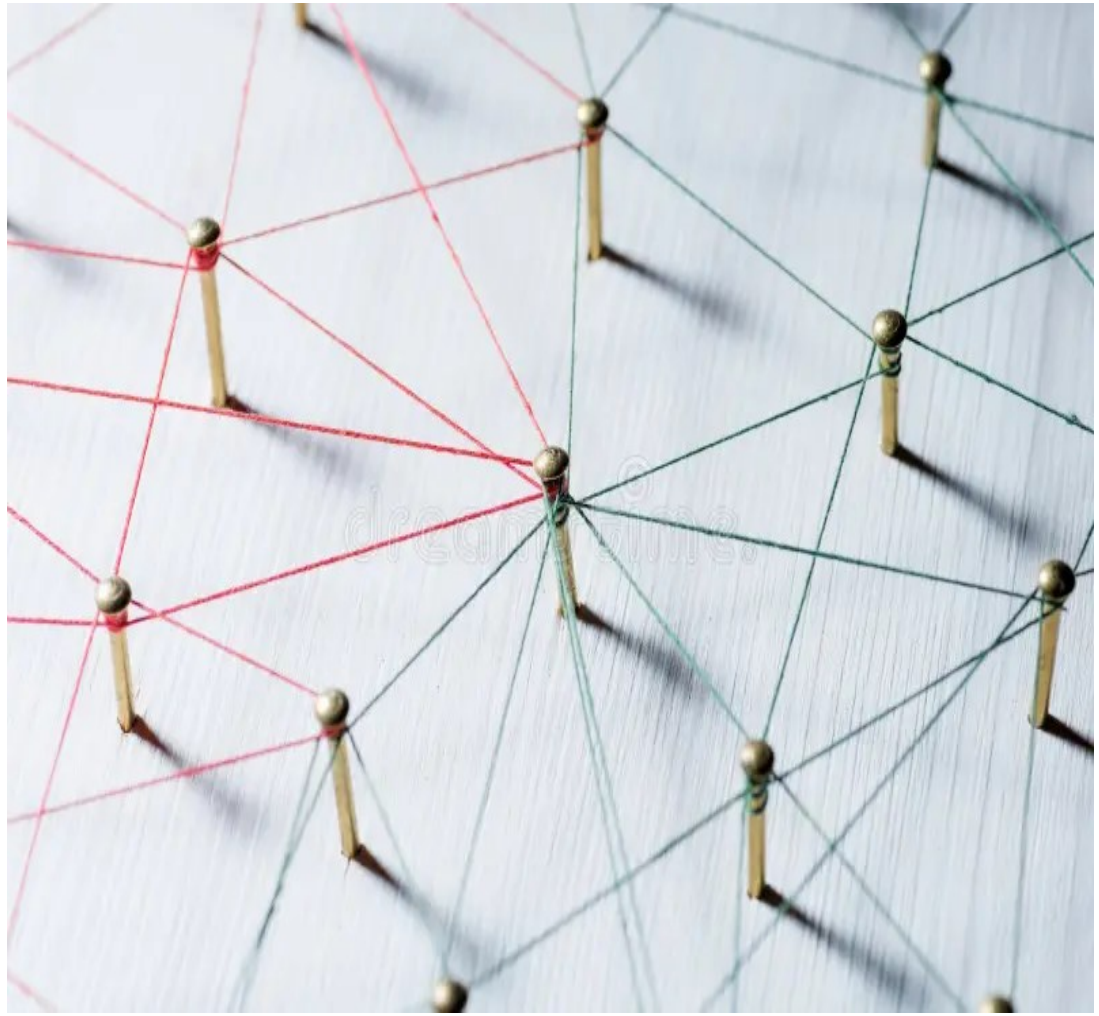
Introduction to Web-Based Threats

What Are Web-Based Threats?

Web-based threats are security risks encountered through the internet, posing dangers to businesses and individuals.

These threats can lead to data breaches, unauthorized access, and system disruptions.

Examples include viruses, phishing attacks, and ransomware.



Co-funded by the European Union

Common Web-Based Threats

Common Types of Web-Based Threats

Attackers impersonate trusted sources via email or messages to steal sensitive data.

Phishing

Malware that encrypts data and demands a ransom for access.

Ransomware

Exploits vulnerabilities in web applications to access or manipulate databases.

SQL Injection

Co-funded by the European Union

Common Web-Based Threats

Common Types of Web-Based Threats

Injects malicious code into trusted websites to compromise user sessions and steal data

Cross-Site Scripting (XSS)

Overloads a server with traffic, making websites and networks unavailable

Distributed Denial of Service (DDoS)

Malicious software that spreads through systems and networks, often damaging data.

Viruses and Worms

CS4ALL
CYBERSECURITY FOR ALL
Co-funded by the European Union

Impact of Web-Based Threats

Effects of Web-Based Threats

Data Breaches

Loss or exposure of sensitive data such as customer information

Financial Losses

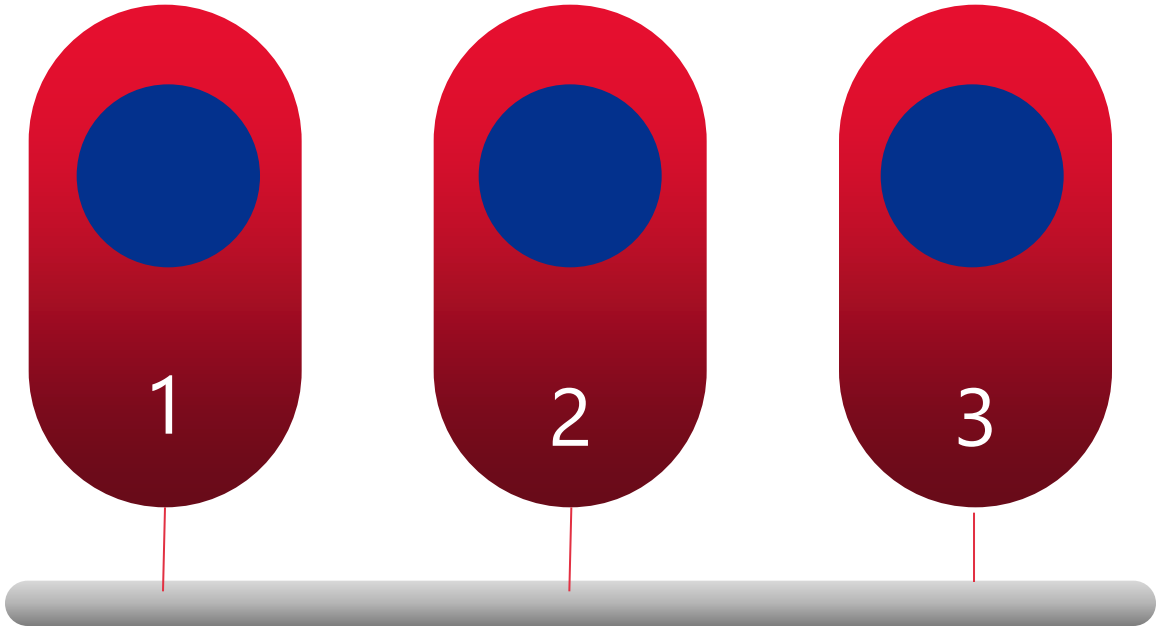
Ransomware attacks, DDoS disruptions, and phishing scams can lead to significant financial costs.

Reputation Damage

Businesses may lose customer trust and credibility after an attack.

Co-funded by the European Union

Preventing Web-Based Threats



Avoid Suspicious Emails and Links

Multifactor Authentication (MFA)

Keep Software Updated

1. Avoid Suspicious Emails and Links

Be cautious when opening unexpected emails or links, as these can lead to malware infections.

2. Multifactor Authentication (MFA)

Enhance account security with additional layers beyond just usernames and passwords.

3. Keep Software Updated

Regularly update antivirus and malware protection softwar

Co-funded by the European Union

Threats and Vulnerabilities

- Understanding Risk
- Threat Agents
- Vulnerabilities

Co-funded by
the European Union

Understanding Risk in Cybersecurity

Risk Equation: Risk = Threats x Vulnerabilities

- Risk refers to the potential for loss or damage when a threat exploits a vulnerability.
- Understanding how threats and vulnerabilities interact to inform effective risk mitigation strategies.

Information Security Risks, Threats and Vulnerabilities

Co-funded by the European Union

Components of a Threat

➢ Threat Agents

Criminals, Hackers, Disgruntled Employees, Political Activists, Commercial Rivals.

➢ Capabilities

Tools, Software, Training, Resources that enhance a threat agent's effectiveness.

➢ Inhibitors

Factors that deter threats, like fear of failure, technical difficulty, law enforcement, or public opinion.

➢ Amplifiers

Elements that escalate threats, such as access to high technology or peer influence.

➢ Catalysts

Events or circumstances that increase the likelihood of a threat, like economic shifts or political events.

CS4ALL
CYBERSECURITY FOR ALL
Co-funded by the European Union

Types of Threat Agents

Natural Agents: Non-human, environmental risks like fire, floods, earthquakes.

Unintentional Agents: Typically internal actors (employees) who may cause damage unknowingly.

Intentional Agents: External or internal, often motivated by hostility, curiosity, or profit. Examples: hackers, spies, organized crime.

Co-funded by the European Union

Top 10 Web Threats

01
- **DDoS Attacks:**
- Increasingly sophisticated, disrupt service by overwhelming servers.

02
- **Browser and Plugin Vulnerabilities:**
- Exploits in outdated software, often in Java, Flash.

03
- **Legitimate Sites with Malicious Content**
- Attackers plant malware on trusted sites (e.g., VOHO attacks).

04
- **Mobile Apps and Unsecured Networks**
- The rise of BYOD (Bring Your Own Device) policies increases vulnerability.

05
- **SQL Injection**
- Top vulnerability, used to manipulate databases.

06
- **Digital Certificate Vulnerabilities**
- Compromised SSL certificates allow for phishing and spoofing

07
- **Cross-Site Scripting (XSS)**
- Used to steal login credentials or manipulate web content.

08
- **Insecure Internet of Things (IoT):**
- Networked devices often lack security updates.

09
- **Automated Bots Scraping Info**
- Used for competitive intelligence, exposes sensitive data.

10
- **Phishing via Familiar Links**
- Exploits people's trust in known sites

Co-funded by the European Union

Vulnerability

Definition: Vulnerabilities are weaknesses or “soft spots” within a network that attackers exploit.

Key Types-

❖ Technology Weaknesses

Issues in protocols, operating systems, or network devices.

❖ Configuration Weaknesses

Misconfigured systems or devices due to human error.

❖ Policy Weaknesses

Weak or poorly enforced security policies.

Co-funded by the European Union

Types of Vulnerabilities

- **Physical Vulnerabilities:** Risks from physical access or damage.
- **Natural Vulnerabilities:** Environmental factors that could disrupt networks.
- **Hardware/Software Vulnerabilities:** Outdated devices, unpatched software.
- **Media Vulnerabilities:** Risks from physical media (disks, tapes) being stolen or damaged.
- **Emanation Vulnerabilities:** Data leakage through radiation.
- **Communication Vulnerabilities:** Weak encryption, unsecured channels.
- **Human Vulnerabilities:** Social engineering, lack of training, or negligence.

CS4ALL
CYBERSECURITY FOR ALL
Co-funded by the European Union

How Vulnerabilities Manifest

- ✓ **External Misuse:** Visual spying, impersonation.
- ✓ **Hardware Misuse:** Eavesdropping, physical tampering.
- ✓ **Masquerading:** Spoofing, network weaving.
- ✓ **Pest Programs:** Trojans, viruses, and worms.
- ✓ **Bypasses:** Trapdoors, unauthorized access.
- ✓ **Active Misuse:** Direct attacks like denial of service.
- ✓ **Passive Misuse:** Interference, data aggregation.

Co-funded by the European Union

Conclusion

Highlights various cybersecurity threats, particularly malware and web-based risks. It discusses different types of malware, such as viruses, worms, ransomware, and spyware, emphasizing their detrimental impacts on systems and data. It also covers social engineering techniques that exploit human psychology to gain unauthorized access to sensitive information, and the serious repercussions these attacks have on individuals and organizations. The chapter concludes with best practices for threats, vulnerabilities and Manifest.

Questions & answers

Invite questions from the audience.

Co-funded by
the European Union

Resources

Research Papers:

1. N. M. Saeed, A. A. Mohammed, and M. A. AlRikabi, "Malware Detection and Prevention Techniques," *Journal of Cybersecurity and Information Systems*, vol. 9, no. 2, pp. 102-115, Jul. 2023.
2. K. Gupta and M. Singh, "Social Engineering Attacks: Techniques and Countermeasures," *International Journal of Cyber Security and Digital Forensics*, vol. 11, no. 3, pp. 45-60, 2022.
3. P. A. Lewis and J. T. Anderson, "Phishing Attacks and Defenses: A Taxonomy," *IEEE Access*, vol. 11, pp. 29384-29395, 2023.
4. R. Chen and M. Zhang, "Ransomware Evolution: From Encryption to Destruction," *Computers & Security*, vol. 128, pp. 89-100, Apr. 2023.
5. A. Patel, S. Mitra, and B. Singh, "Cross-Site Scripting (XSS) Vulnerabilities: Detection and Mitigation Strategies," *ACM Trans. Internet Technol.*, vol. 22, no. 1, pp. 13-23, Dec. 2022.

Books:

1. M. Ligh, A. Case, and J. Levy, *Malware Analysis Techniques*, 2nd ed., New York, NY, USA: Wiley, 2022.
2. C. Hadnagy, *Social Engineering: The Science of Human Hacking*, 3rd ed., Hoboken, NJ, USA: Wiley, 2023.
3. N. R. Jennings, *Cybersecurity Threats, Malware Trends, and Strategies*, 1st ed., London, UK: Springer, 2023.
4. C. Hadnagy, *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails*, 2nd ed., Indianapolis, IN, USA: Wiley, 2021.
5. A. Hoffman, *Web Application Security: Exploitation and Countermeasures for Modern Web Applications*, 1st ed., Sebastopol, CA, USA: O'Reilly Media, 2023

Co-funded by the European Union