training code: E-CYBER / ENG e-learning / EN

Cybersecurity in Practice: How to Protect Yourself and Your Organization

E-learning will be available starting in June 2026.

The "Cybersecurity in Practice: How to Protect Yourself and Your Organization" training is an interactive online course designed to help you protect your data, avoid threats, and respond effectively to cyberattacks- regardless of your technical knowledge level.

You can complete the course at your own pace and at any time in a convenient self-learning format. It is a practical tool that will help you build strong personal cybersecurity habits.

The training consists of five thematic modules. Each module includes knowledge-check quizzes, and the entire course uses a variety of multimedia techniques, interactive exercises, and real-world scenarios to ensure effective learning and maximum engagement.

Training recipients

This training is designed for all employees across the organization, regardless of department or technical experience. It is particularly beneficial for individuals who:

- use computers and smartphones in their daily work,
- have access to company or customer data,
- are interested in strengthening their digital skills and protecting their online privacy.

This training is not just a requirement- it’s a real value and an investment in both your personal security and your organization’s cybersecurity

Benefits

Benefits for Participants

- Recognizing Online Threats- You will learn how to identify and avoid phishing attacks, malware, and social engineering attempts.
- Password Management- You will understand how to create strong, unique passwords and manage them securely.
- Understanding Cybercriminal Tactics- You will learn common hacking techniques and how to effectively respond to attempted cyberattacks.
- Backup Creation- You will master best practices for creating backups and understand their critical role in data protection and recovery.
- AI Threat Awareness – You will learn how to recognize deepfakes and other forms of digital disinformation associated with the advancement of artificial intelligence.

Benefits for the Organization

- Reduced Cyber Incident Risk- Minimize the likelihood of successful cyberattacks, fraud, and data breaches.
- Building a Security Culture- Strengthen employee awareness of cyber threats and increase engagement in protecting organizational assets.
- Protection of Company Reputation and Data- Safeguard sensitive information from unauthorized access and prevent costly reputational crises.
- Reduction of Human Error – Decrease the number of incidents caused by lack of knowledge or employee inattention.
- Resilience to Emerging Digital Threats- Prepare the organization to respond effectively to rapidly evolving threats, including those related to artificial intelligence and disinformation

Training program

The training consists of five thematic modules covering key aspects of cybersecurity:

Module 1: Fundamental Cyber Threats

- Phishing and spear phishing
- Ransomware
- Malware (viruses, trojans, spyware)

Module 2: Password and Identity Security

- The importance of strong passwords and identity management
- Best practices for creating secure passwords
- Password management methods (including password managers)
- Common methods of password compromise
- Fundamental password security principles

Module 3: How Attacks Happen – Hacker Techniques

- Overview of attack vectors and social engineering methods
- Risks associated with the Internet of Things (IoT)
- Defensive strategies and best practices for preventing attacks

Module 4: The Importance of Backups

- The role and purpose of backups
- Types of backups and backup methods
- The importance of regular backups for data protection and recovery

Module 5: The (In)Security of Artificial Intelligence (AI)

- AI-related threats (deepfakes, fake images, generated text)
- Methods for recognizing disinformation and manipulated content

Expected preparation of the participant

It is not required.

Duration

1 days / 2 hours

Language

English