Cybersecurity and AI

Between Threats and Best Practices

Duration: 3 hours
Prerequisites:
- No prior knowledge of cybersecurity required.
- Access to a computer with an Internet connection.

Teaching methods:
- Online training, asynchronous
- Training materials included

Skills acquired by the end of the course:
- Understand how generative AI tools work and where their risks lie
- Recognize AI-powered cyberattacks
- Use and configure AI tools securely

Certificate: yes

DESCRIPTION

Artificial intelligence (AI) offers considerable benefits to organizations, but it is also exploited by cybercriminals. In this course we explore the methods currently used to turn AI to criminal ends, and provide recommendations for using AI securely in our professional activities.

PROGRAM:

General objective

Raise participants' awareness of the security risks associated with AI. Teach best practices for the secure use of AI in the workplace.

1. Introduction to Artificial Intelligence and Its Practical Applications — The evolution of AI in the technology field. Understanding how generative AI models work. An overview of the popular tools (ChatGPT, Gemini, Copilot, Claude, etc.). Examples of AI use in a professional context.

2. Current Trends in AI-Powered Cyberattacks — Examples of attacks using AI (deepfakes, automated phishing, fraudulent content generation, ransomware creation). Understanding deepfakes and AI-enabled identity theft. Tools for detecting deepfakes and fraud (machine learning, anomaly detection). Case studies and simulations to strengthen prevention against sophisticated attacks.

3. How AI Platforms Work — Distinguishing personal use from professional use. Understanding data processing and learning models. Clarifying where data is hosted and what that means for the protection of personal information.

4. Data Management Challenges — Considerations related to the protection of personal information. Best practices for anonymizing information in prompts. Intellectual property issues around content generated or submitted. Understanding the limits of these systems, including hallucinations and possible errors. Awareness of bias in AI models (racial, gender) and its impacts.

5. Settings and Best Practices — Privacy settings and history management. Possible reuse of data to train models. Exploring « private » AI. Recommendations for the secure use of AI tools across the organization.

QUESTIONS/ANSWERS