Strategic business protection in the age of AI

Course code: AI_DIGITALSEC

This course is aimed at providing practical knowledge and skills in protecting against digital manipulations such as deepfake and fake news. You will learn not only how to identify manipulations, but also how to implement measures to prevent and respond effectively to these threats. This course is ideal for corporate employees who want to protect themselves and their organisation from modern digital risks.

Who is the course for

This course is designed for corporate employees who want to improve their digital security and learn how to identify and respond to digital content manipulation. It is suitable for all levels of employees, from beginners to managers who work with sensitive data and information.

What we teach you

- Identify deepfake videos and fake news articles.
- Recognize manipulation in text, images and audiovisual materials.
- Establish safe habits for working with digital media.
- Respond to digital attacks and manipulations in real time.
- Establish internal guidelines and protocols for digital security.
- Utilize available tools to detect deepfakes and misinformation.

Required skills

- Basic computer and internet skills.
- Experience with corporate systems an advantage but not a requirement.

Course outline

Introduction to digital security
- What is deepfake and fake news.
- How they are created and why they are dangerous.
- The impact of digital manipulation on companies and individuals.

Techniques for identifying manipulation
- Recognising key deepfake signals in videos.
- Text and image analysis: synthetic and manipulated content.
- Verification of information sources.

Implementing preventive measures
- Safe habits for working in online environments.
- Setting internal policies and guidelines.
- Staff training: digital literacy basics.

Practical examples and tools for detection.
- Creating deepfake and fake news
- Overview of deepfake detection software.
- Working with tools such as Deepware, Wasit.
- Testing manipulations with real examples.

Responding to digital attacks
- Protocols for reporting and responding to manipulations.
- Communication strategies in case of a deepfake attack on a company.
- Practical steps to restore trust and ensure security.

Ethics and legislation
- Legal framework for protection against digital manipulation.
- Ethical boundaries when working with digital media.

GOPAS

- The future of deepfake and fake news regulation.
- EU AI Act
- The view of the Czech courts