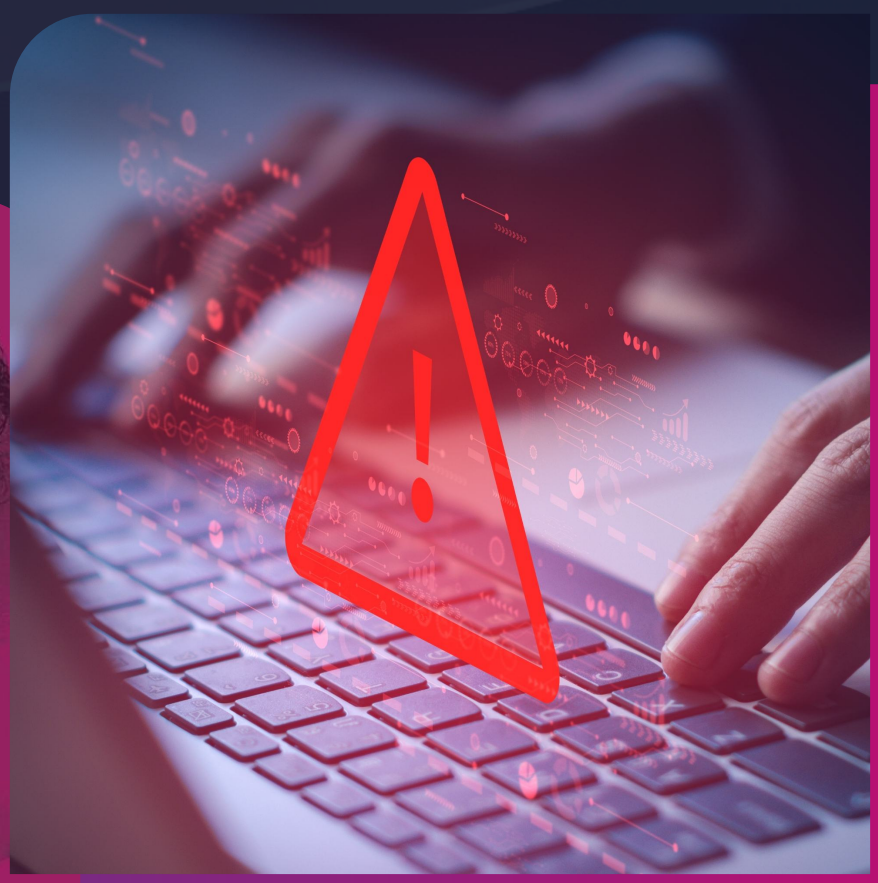
Digital 4 Business
Evolving your digital future

Cybersecurity for Business

Become a cybersecurity expert and secure digital data systems



4

Equip yourself with advanced techniques to counteract emerging cyber threats.

Master techniques to protect against evolving cyber threats. This module equips you to safeguard both personal and organisational data. Learn to detect vulnerabilities and prevent breaches in data systems. Create effective protection measures to keep your data secure from future threats.

Discover the ethical and legal complexities of cybersecurity, and gain the confidence to navigate this rapidly changing field. Become a key player in digital security today, ready to handle tomorrow's challenges.

Learning objectives

This module equips students to detect vulnerabilities, craft protection strategies, and understand cybersecurity's legal and ethical aspects. By the end, you'll have learned to:

Examine and assess weaknesses in data systems to identify potential breaches and propose solutions to prevent them.

Implement advanced cyber attack strategies to simulate breaches, gaining deep insights into cybersecurity threats.

Create and execute comprehensive data protection methods using encryption and advanced security protocols.

Evaluate and use sophisticated tools to both identify and respond to cyber threats, staying proactive against future risks.

Critically assess and debate cybersecurity legal and ethical issues, formulating well-justified recommendations for policy and practice that reflect an advanced understanding of the complexities and responsibilities in the field of cybersecurity.

Criteria — are you eligible?

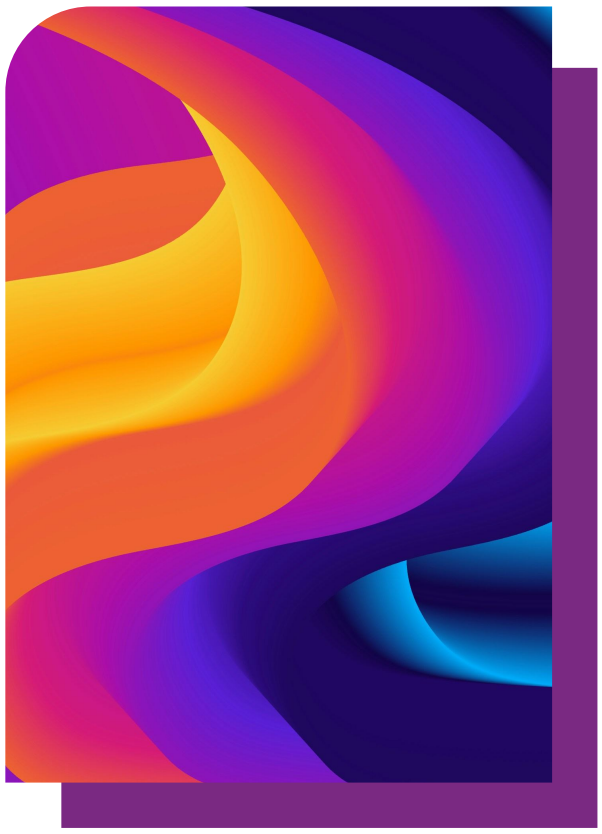
- **Language proficiency:** Minimum C1 English proficiency, plus 2 years' work or education in an English-speaking environment. IELTS: 6.0; TOEFL PBT: 600; TOEFL CBT: 200; TOEFL iBT: 100
- **Education:** Relevant EQF Level 6 qualification required (eg STEM, economics). Without this you will have an interview and assessment to evaluate certifications, qualifications or professional experience.
  **EQF levels explained*
- **Residency:** This EU-funded programme is open to all EU nationals with a passport or valid ID from one of the 27 EU countries.

Cybersecurity for Business

Unlock new cybersecurity career paths

The Digital4Business Cybersecurity module is designed for IT professionals and tech enthusiasts who want to progress in digital security. It opens doors to careers in cybersecurity analysis, ethical hacking, data protection and more.

Our Master's programme as a whole includes a wide range of complementary modules to enhance your learning.



Advanced online learning with expert guidance and emerging tools

This online module employs an innovative hybrid learning model, offering live lectures, self-paced study, and hands-on lab sessions with the guidance of expert tutors. You'll experience problem-based learning, gamification, and flipped classroom strategies, enhanced by artificial intelligence to enrich your education.

Assessments are continuous and final, involving exams, projects and assignments. Half of the assessment involves applying cybersecurity to real-world business issues, and the remaining 50% tests your comprehensive understanding of the subject.

Time commitment

- Classroom and demonstrations: 36 hours
- Practical work/tutorials: 24 hours
- Independent learning: 190 hours
- Total: 250 hours

Credit points

- 10 ECTS

Full course content

Subjects covered

Cybersecurity for Business is a 10 ECTS module with 5 hours per week, over 12 weeks. The following schedule outlines the topics covered each week:

- **Introduction to Cybersecurity**
  - Overview of cybersecurity, its importance, and the growing demand for professionals
  - Understanding online identity, data, and their significance to cybercriminals
  - Seminar on real-world cybersecurity challenges
- **Risk Management and Compliance**
  - Exploring the significance of safeguarding electronic information networks and data
  - Regulatory compliance requirements for business
  - Implementing risk assessments and developing risk mitigation strategies
  - Lab on security breach case studies
- **Network Security for Business**
  - Addressing software and hardware vulnerabilities, device, network, and cloud security
  - Implementing secure network infrastructure including best practices for securing wireless networks and remote access
  - Lab on securing the application landscape, incident response planning and security incidents management
- **Cyber Attacks: Concepts and Techniques**
  - Analysis of cyberattacks, identifying and classifying security vulnerabilities
  - Understanding endpoint security challenges in business environments
  - Securing IoT devices and other connected endpoints in business networks
  - Seminar on vulnerabilities and real-world use cases
- **Data and Privacy Protection**
  - Best practices for protecting computer devices, wireless networks, and online accounts
  - Implementing cryptographic methods for business data
  - Exploration of ethical implications and considerations in using AI and cryptography for data privacy protection
  - Practical exercises on implementing cryptographic techniques for privacy-preserving data sharing and analysis
  - Lab on data encryption and backup strategies
- **Organisational protection and cloud security for business**
  - Techniques for firewall configuration, port scanning, and certificate updates
  - Securing cloud services and data storage in public, private, and hybrid cloud environments
  - Identity and access management in the cloud
  - Data backup and disaster recovery planning for cloud-based systems
  - Lab on using tools for security monitoring
- **Cyberattack Detection and Cyberdefense**
  - Real-time attack detection, best security practices, and understanding botnets and the kill chain
  - Lab on behaviour-based security
- **Tools for incident prevention and detection**
  - Overview of CSIRT, security playbooks, IDS, and IPS
- **Cybersecurity Legal Issues**
  - Personal legal issues. Corporate Legal Issues.
  - International Law and Cybersecurity
- **Ethical Issues in Cybersecurity**
  - Overview of cybersecurity laws, regulations, and industry standards applicable to businesses
  - Understanding ethical considerations in cybersecurity decision-making
  - Addressing legal and ethical challenges related to incident response, data breaches, and privacy violations
  - Discussion on ethical considerations and the role of professional organisations in cybersecurity ethics
- **Cyberwarfare**
  - Understanding cyberwarfare, its objectives, and impacts
- **Emerging Topics and Careers in Cybersecurity**
  - Exploration of AI in cyberattacks and defence, the geopolitical aspects of cyberspace, and blockchain technology