Course Information Sheet

BSc (Hons)

Cybersecurity with Artificial Intelligence

Mode and course length – Full-time (3 years)

Location – UCLan London campus (East India Docklands)

Awarding Body – University of Lancashire. As a registered Higher Education provider University of Lancashire is regulated by the Office for Students.

UCLan London

Overview

This course is designed to equip students with strong theoretical knowledge and applied technical skills in cybersecurity, enhanced through the integration of artificial intelligence. The programme reflects the growing importance of cybersecurity in protecting digital systems, infrastructure and data across all sectors.

Throughout the course, students will develop expertise in areas including computer systems and networks, programming for cyber security, digital forensics, software security, security operations, ethical hacking, governance, risk and compliance, and applied AI for cyber security. Students will engage in lab-based activities, simulated cyber scenarios and real-world case studies, enabling them to apply theoretical knowledge in practical contexts.

Course Delivery

Our courses are delivered through a variety of teaching and learning methods that provide students with a modern and engaging higher education experience. These include lectures, seminars, workshops, practical sessions, group projects, reflective practice, case studies, and work-related learning. You will also use our Virtual Learning Environment (VLE) to access learning resources, submit assignments, and engage in online discussions.

Each course is structured into 'modules', each focusing on specific subject areas. Module information, including learning outcomes and assessment requirements, will be provided through Module Handbooks and the VLE.

Assessment

Assessment methods are varied and may include written assignments, essays, case study analyses, presentations, reports, health promotion campaigns, reflective logs, and research projects. These approaches allow you to demonstrate both your academic knowledge and your practical skills.

Most modules include more than one assessment, giving you the opportunity to develop a range of competencies. Formative feedback will be provided throughout your studies to help you progress and strengthen your performance.

Fees

Information about your course fee, including any annual fee increases or deposits (if required), can be found in your offer letter.

Additional Costs

During your course, you may be required to take extra or repeated modules to recover any modules you have failed. You will be charged an additional tuition fee to cover the costs of the extra or repeat modules. This additional fee will be based on the credits for the module(s) you repeat or take.

Modules

Core Modules

Year 1: CO1025 Computer Systems and Networks

This module aims to develop students' foundational understanding of computer systems and networked environments, with particular focus on how digital systems are structured, connected and operated in contemporary computing contexts. It introduces the core principles of computer architecture, operating systems, networking models, protocols and infrastructure, and supports students to understand how these elements function together in practice.

The module emphasises technical understanding, interpretation and application rather than advanced system administration or specialist cybersecurity analysis, preparing students for later study in cybersecurity, programming, cryptography, security operations and ethical hacking.

Year 1: CO1026 Programming for Cyber Security

This module aims to introduce students to fundamental programming concepts and their application within cybersecurity contexts. It develops students' understanding of how programming supports problem-solving, automation, data handling and technical analysis in contemporary digital environments.

The module also aims to build students' confidence in writing, testing and evaluating simple programs, while developing logical thinking, computational problem-solving and an appreciation of how programming supports later study in software security, data and AI for cyber security, ethical hacking and related technical areas.

Year 1: CO1027 Cyber Security Fundamentals

This module aims to provide students with a foundation in the key principles, concepts and practices of cybersecurity within contemporary digital environments. It introduces the nature of cyber threats, vulnerabilities, risks and controls, and supports students in developing an understanding of how systems, networks and information can be protected in practice.

The module also aims to develop students' awareness of legal, ethical and professional responsibilities in cybersecurity, while introducing the role of basic security tools, defensive approaches and emerging technologies such as artificial intelligence. It prepares students for later study in more specialised areas of cybersecurity, including cryptography, digital forensics, security operations and ethical hacking.

Year 1: CO1028 Data and AI for Cybersecurity

This module aims to introduce students to the role of data and artificial intelligence in contemporary cybersecurity practice. It develops students' understanding of how security-relevant data is generated, collected, processed and analysed, and how data-driven and AI-influenced approaches can support cybersecurity decision-making.

The module also aims to build students' ability to work with basic cybersecurity datasets, apply

introductory analytical techniques, and critically evaluate the benefits, limitations and risks of artificial intelligence in cybersecurity contexts. It prepares students for later study in applied AI, security operations and related technical modules.

Year 2: CO2031 Applied Cryptography

This module aims to provide students with a comprehensive understanding of cryptographic principles and their practical application in securing modern information systems. Students will develop the ability to evaluate, implement, and analyse cryptographic techniques used to ensure confidentiality, integrity, authentication, and non-repudiation.

The module introduces both classical and modern cryptographic systems and explores their applications in real-world scenarios, including secure communication, digital signatures, and blockchain technologies. Students will also gain awareness of current challenges and vulnerabilities in cryptographic systems, preparing them for roles in cybersecurity and secure system design.

Year 2: CO2032 Digital Forensics

This module introduces students to the core principles and practices of digital forensics within investigative and organisational settings. It develops understanding of how digital evidence is identified, collected, analysed and presented to support investigations. Topics include the forensic lifecycle, legal and ethical frameworks, evidence acquisition, digital forensics analysis and profesing. Students will apply forensic techniques and tools to examine digital artefacts and reconstruct user and system activities, developing practical investigation skills and the ability to produce structured reports that communicate investigative findings.

Year 2: CO2033 Software Security

This module introduces students to the core principles and practices of software security within modern software development contexts. It develops understanding of how software security risks arise and how security can be integrated throughout the software development lifecycle. Topics include software vulnerabilities, secure design and coding practices, threat modelling, security testing and ethical and legal considerations. The module develops students' analytical and critical evaluation skills, enabling them to assess software security decisions and recommend informed improvements aligned with ethical and legal responsibilities.

Year 2: CO2034 Security Operations

This module develops a comprehensive understanding of security operations within organisations, focusing on the processes, technologies and practices used to detect, monitor and respond to cyber threats. You will explore the role of Security Operations Centres (SOCs), including threat intelligence, security monitoring, incident detection and response, and vulnerability management.

The module introduces key operational tools and techniques such as Security Information and Event Management (SIEM), log analysis, and automation within security operations. It will also enable you to analyse real-world security scenarios and apply structured approaches to incident handling and reporting. Furthermore, the module examines the importance of communication, governance, and ethical considerations in security operations, drawing from

relevant professional frameworks such as the Cyber Security Body of Knowledge (CyBOK). The module builds on prior knowledge from Computer Systems and Networks and prepares students for practical roles in cybersecurity operations environments.

Year 3: CO3028 Individual Project

This module aims to enable students to plan, undertake and present an independent honours-level project in a cybersecurity-related area. It develops students' ability to define a focused project problem or investigation, synthesise and evaluate relevant literature and evidence, justify an appropriate technical, analytical or research-informed approach, and complete a substantial piece of independent work.

The module also aims to support students to critically analyse and evaluate project processes, outputs and findings, and to produce well-structured conclusions and recommendations relevant to cybersecurity practice, investigation, development or analysis.

Year 3: CO3029 Applied AI in Cybersecurity

This module develops advanced, practice-focused understanding of how artificial intelligence and machine-learning techniques are applied within contemporary cybersecurity operations and analytical workflows.

Year 3: CO3030 Governance, Risk, and Compliance

This module provides an in-depth examination of Governance, Risk Management, and Compliance (GRC) within contemporary digital organisations. It develops your ability to critically evaluate governance frameworks, assess organisational risk, and ensure alignment between cyber security practices and strategic objectives.

Year 3: CO3031 Ethical Hacking

This module aims to develop students' advanced knowledge and practical skills in ethical hacking and penetration testing. Students will learn to identify, exploit, and assess vulnerabilities in systems, networks, and applications in a controlled, ethical manner. The module focuses on real-world offensive security techniques and tools used by professionals to evaluate system security.