UNIVERSITY OF LIVERPOOL

CYBER SECURITY

we are the original redbrick

The University of Liverpool works with partner, Kaplan Higher Education Hong Kong, to process applications and admissions.

CYBER SECURITY

Programme overview

Study mode: Online and part-time

Qualification: MSc / PG Dip / PG Cert Cyber Security

Indicative programme duration: 24 months / 16 months / 8 months

The study duration of this programme is currently subject to change and final validation.

Accreditation(s): The programme is accredited by the BCS, The Chartered Institute for IT, for the purposes of meeting the further learning academic requirement for registration as a Chartered IT Professional.

Entry requirements: Applicants should possess either:

- A degree in any subject^ equivalent to a UK Bachelor's degree of 2:2 or above; or
- At least two years' work experience, ideally of a technical nature, comparable with a Bachelor's degree

All applicants must provide evidence that they have an English language ability equivalent to an IELTS (academic) score of 6.5 overall (5.5 in all components).

Applications from under-represented groups within the Computer Science/IT industry will be particularly welcome.

Teaching and assessment

The programme is delivered using the latest and most innovative online teaching techniques and includes a range of interesting and thought-provoking activities and exercises. Core information is developed by subject-leading experts in the field and closely aligned with both industry and academic best practice, underpinned by rigorous theoretical and relevant topics, examples and cases. Leading-edge materials are supported by specially trained tutors, who are not only professionals in the discipline, but who have an exceptional knowledge of supporting online students. Teaching activities consist of specially designed lecturecasts, carefully curated reading lists, and asynchronous discussions to enhance peer-to-peer learning opportunities.

Assessment is by coursework only – there are no examinations. Assessments align with the University of Liverpool commitment to have relevant, authentic and varied activities and are designed to lead directly to enhanced professional and personal objectives as well as being appropriate to the academic discipline.

*The indicative study duration is a guide to how long your course will take to complete. The actual duration may vary depending on study options chosen and module availability.

^Candidates with more limited exposure in numeracy or programming may need to consider further effort in these areas to maintain the standards of the programme.

Ready to apply? Please complete our online application form to apply to study this programme.

CYBER SECURITY

What will I study?

This programme consists of the following modules. You are required to complete 180 credits to achieve a full Master of Science, 120 credits to achieve the postgraduate diploma (PG Dip), and 60 to achieve the postgraduate certificate (PG Cert).

	MSc	PGDip	PGCert
Global Trends in Computer Science (15 credits)	*	*	*
Security Engineering and Compliance (15 credits)	*	*	*
Cyber Crime Prevention and Protection (15 credits)	*	*	*
Networks and Web Technology (15 credits)	*	*	*
Cyber Forensics (15 credits)	*	*	
Security Risk Management (15 credits)	*	*	
Choose one elective module from (15 credits): Applied Cryptography Multi-Agent Systems Software Development in Practice Databases and Information Systems	*	*	
Research Methods in Computer Science (15 credits)	*	*	
Computer Science Capstone Project (60 credits)	*		

Ready to apply? Please complete our online application form to apply to study this programme.

UNIVERSITY OF LIVERPOOL

PROGRAMME STRUCTURE

Module code	CSCK501	**NQF level**	Level 7
Credit value	15 credits	**Module duration**	8 weeks

GLOBAL TRENDS IN COMPUTER SCIENCE

Module aims

This module aims to:

- Familiarise students with the online classroom environment and allow them to explore current practice in computer science and information technology by sharing their global perspectives and experiences in discussion forums.
- Provide a comprehensive and holistic introduction to current trends in computer science, such as enterprise systems management, data protection and big data analytics, cyber security, pervasive computing, sustainable technology and risk management.
- Highlight the global, integrative and collaborative nature of the information technology industry, whilst allowing students to explore the relevance and impact of their unique regional contexts through critical discussion and group work.
- Allow students to explore and critically debate the use of information technology in an enterprise setting, the best way to make decisions regarding technology, and the management and administration needs of an organisation.

Learning outcomes

Students will be able to:

- Contribute to an academic community via the use of an online classroom and discussion forum, whilst demonstrating a commitment to lifelong learning, academic integrity and an understanding of the academic writing style.
- Produce an artefact that involves searching for, assimilating and analysing relevant scholarly resources, reflecting a range of viewpoints with original thought and commentary, and demonstrating digital fluency with search tools and presentation software.
- Demonstrate a critical understanding of current trends in computer science, and an appreciation of how information technology can be used to support business processes and add value to global enterprises.
- Articulate the legal, social, ethical and professional issues related to developing and using information systems and modern technology solutions, demonstrate professionalism, and follow relevant professional codes of practice.

Syllabus

- Trends in computer science
- Information technology
- Data and risk management
- Cyber security
- Green computing
- Internet of things and smart cities
- Big data analytics
- Real-time, high integrity and embedded systems

MSc / PG Dip / PG Cert

Module code	CSCK509	**NQF level**	Level 7
Credit value	15 credits	**Module duration**	8 weeks

SECURITY ENGINEERING AND COMPLIANCE

Module aims

This module aims to:

- Provide students with a critical understanding of information security concepts and models.
- Provide students with a comprehensive appreciation of threats, attacks and vulnerabilities on information systems and critical infrastructures.
- Provide students with a systematic critical understanding of security compliance and industry standards.
- Equip students with the ability to identify, evaluate and apply information security models and protocols to solve security problems in the work place.
- Develop the ability of students to: carry out security and risk assessments, to design and deploy security infrastructures, write security/ incident response polices and to conduct penetration testing.

Learning outcomes

Students will be able to:

- Develop an in depth and critical understanding of information security concepts and models.
- Develop an in depth and wide-ranging understanding of the principles and best practices for protecting information systems and critical infrastructures through prevention, detection and response cycles.
- Develop a wide-ranging capability to identify threats, design security infrastructures and defeat attacks on information systems.
- Develop a comprehensive ability to develop security compliance policies according to industry standards.
- Develop a substantial capability to carry out penetration testing and perform risk assessment for an organisation.

Syllabus

- Information security concepts such as confidentiality, integrity, authenticity and availability.
- Security models (such as privacy models and integrity models) and security policies in the context of cyber security.
- Network security, wireless security, mobile security, Internet of Things security and infrastructure security.
- Security compliance, industry standards and industry recognition.
- Risk analysis and risk assessment.
- Firewalls and intrusion detection systems.
- Software testing, security penetration testing and quality assurance.
- Digital content protection in the context of cyber security compliance.

Module code	CSCK510	**NQF level**	Level 7
Credit value	15 credits	**Module duration**	8 weeks

APPLIED CRYPTOGRAPHY

Module aims

This module aims to:

- Provide students with an in-depth understanding of symmetric key encryption algorithms, hash function algorithms, public key cryptography algorithms and key agreement protocols.
- Equip students with a comprehensive understanding of attacks and vulnerabilities with respect to current industrial standards for cryptography.
- Provide students with a wide-ranging understanding of quantum computing techniques and the ability to evaluate their impact with respect to the security of current cryptographic techniques.
- Provide students with the ability to evaluate and apply cryptographic algorithms and protocols to solve cyber security problems (such as confidentiality, integrity and authenticity problems) in the work place.
- Develop the competence of students to identify, select and adapt open source cryptographic techniques to design and implement secure software products, for commercial and non-commercial usage.

Learning outcomes

Students will be able to:

- Develop an in depth and critical understanding of cryptographic algorithms for symmetric encryption schemes, secure hash functions, public encryption schemes and digital signature schemes.
- Develop a systematic appreciation of the limitations of current cryptographic schemes in the quantum computing era, and a substantial understanding of post-quantum cryptographic techniques.
- Develop a wide-ranging capability to assess and use cryptoanalytical software/hardware applications, and to carry out ethical hacking on cryptographic protocols within deployed Internet applications.
- Develop a comprehensive ability to develop secure software products using open source tools.
- Develop a substantial capability to evaluate and apply cryptographic algorithms, and authentication, identification and zero knowledge protocols, so as to be able to design secure commercial applications (such as secure Internet of Things applications).

Syllabus

- Introduction to classical cryptography
- Block ciphers, symmetric key encryption and secure hash functions.
- Public key cryptographic encryption and signature schemes.
- PKCS: Public Key Cryptography Standards.
- Elliptic Curve cryptography.
- Quantum computing and quantum cryptography.
- Key agreement, identification and zero-knowledge.
- Password authentication, identity based cryptography and other advanced topics.

Module code	CSCK511	**NQF level**	Level 7
Credit value	15 credits	**Module duration**	8 weeks

CYBERCRIME PREVENTION AND PROTECTION

Module aims

This module aims to:

- Provide students with a wide ranging understanding of the information security management landscape.
- Equip students with a comprehensive knowledge and understanding of the potential of cybercrime (through ethical hacking).
- Provide students with systematic understanding of the tools and techniques that can be deployed for cybercrime prevention.
- Develop the practical ability of students to deploy the tools and techniques of cybercrime prevention in both commercial and non-commercial settings.

Learning outcomes

Students will be able to:

- Develop a comprehensive understanding of the cyber-crime prevention "landscape", including the tools and techniques available to mitigate against the effects of cybercrime.
- Develop an in depth and critical understanding of the concepts of ethical hacking and information security management.
- Develop a comprehensive ability to analyse computer security problems as well as being able to identify and define countermeasures appropriate to their solution.
- Develop a substantial ability to cooperate effectively in teams to address common cybercrime prevention issues, especially in the context of asset protection.
- Develop an in depth understanding of smartphone security and the associated protection issues.

Syllabus

- Critical overview of cybercrime prevention terminology and the legal aspects involved.
- Information security management, security auditing, monitoring, ethical hacking and penetration testing.
- Building of an ethical hacking environment (laboratory) to allow experimentation with hacking techniques in weeks 4 and 5, so that a comprehensive understanding of these techniques can be gained.
- Ethical hacking in a number of contexts such as: wireless communication, Wi-Fi Protocol access, Operating Systems, the " Secure Sockets Layer" , access point cloning, router attacks, SQL injection and the building of key loggers.
- Techniques, tools and processes for cybercrime prevention in a variety of domains such as: desktop applications, wireless access points, smartphones and bluetooth connections.
- Comprehensive understanding of the security challenges of emerging computing environments.

Module code	CSCK512	**NQF level**	Level 7
Credit value	15 credits	**Module duration**	8 weeks

CYBER FORENSICS

Module aims

This module aims to:

- Provide students with a comprehensive understanding of the domain of computer forensics.
- Instruct students in the tools and techniques that will allow them to identify and extract evidence from computer media.
- Equip students with an in depth knowledge of the processes whereby material extracted from computer media can be assessed and judged for evidentiary purposes.
- Provide students with a complete understanding of the process of documenting computer forensic evidence.

Learning outcomes

Students will be able to:

- Develop a deep and critical understanding of the theory and practice of computer forensics.
- Develop a complete understanding of the processes for digital evidence acquisition, authentication, analysis, and auditing.
- Develop an understanding of the use of computer forensic tools to carry out digital forensic investigation.
- Conduct digital forensic investigations with respect to a variety of computer platforms.
- Develop an understanding of the legal framework within which the discipline of computer forensics operates (with respect to a number of different countries).
- In the context of computer forensics, differentiate between ethical issues, legal issues, and criminal motives.
- Develop an awareness of future trends in computer forensics.

Syllabus

- Digital Evidence, Computer Crime, Technology, and Law
- The Investigative Process, Reconstruction, and Modus Operandi
- Applying Forensic Science to Computers
- Investigating Windows Computers and Network Forensics
- Investigation Unix Systems, Macintosh Systems, and Handheld Devices
- Network Forensics I
- Network Forensics II
- Computer Crime Investigation and Career Development

Module code	CSCK551	**NQF level**	Level 7
Credit value	15 credits	**Module duration**	8 weeks

SECURITY RISK MANAGEMENT

Module aims

This module aims to:

- Provide students with theoretical and practical knowledge of the domain of (Cyber) Security Risk Management, along with an insight into the formal and systematic approaches core to Security Risk Management.
- Provide students with a substantial technical awareness, and managerial competence, concerning information security policy and management.
- Provide students with advanced knowledge of the security issues that can affect information and computer systems.
- Provide students with practical ability in the application of the concepts, techniques, methods and approaches of Security Risk Management in the context of enterprises of all kinds.

Learning outcomes

Students will be able to:

- Develop an ability to analyse and assess (Cyber) Risk Management scenarios by utilising systemic analysis processes.
- Develop a systematic ability develop and deploy a program of Cyber Security using the tools and techniques of security risk management.
- Develop an in-depth and critical understanding of the professional codes of practice, and legal, social, cultural and ethical issues, related to security risk management.
- Develop a comprehensive awareness of the social and environmental context in which security risk management operates .
- Develop the practical ability to apply the tools and techniques of security risk management, in a manner that is both practical and pragmatic, and in the context of enterprises of all kinds.

Syllabus

- The principles of (Cyber) Security Risk Management.
- Security Risk management, management models, roles, and functions.
- Strategic management planning and strategies, the security management life cycle.
- Laws and regulatory requirements concerning cyber security, and security standards and controls.
- Security metrics and Key Performance Indicators (KPIs).
- Physical security and environmental threats, contingency planning.
- Security training and awareness, the creation of a security staff training plan.
- The future of Cyber Security Risk Management; the potential impacts of evolving technologies.

Module code	CSCK504	**NQF level**	Level 7
Credit value	15 credits	**Module duration**	8 weeks

MULTI-AGENT SYSTEMS

Module aims

This module aims to:

- Provide students with a thorough and comprehensive understanding of the computer science domain of multi-agent systems.
- Enable students to critically evaluate current theories and methods in multi-agent system design and their application to a wide variety of contexts.
- Equip students with technical knowledge and skills to develop and deploy multi-agent system solutions to solve real world problems.

Learning outcomes

Students will be able to:

- Demonstrate an in-depth understanding of the area of multi-agent systems, their theoretical underpinning and practical applications.
- Demonstrate a comprehensive understanding of the difference between the multi-agent paradigm and the more conventional approaches to complex systems design.
- Analyse real world problems for which a multi-agent system approach is appropriate, and formulate a solution.
- Critically evaluate and deploy software tools and skills for the implementation of multi-agent systems.

Syllabus

- Agents, objects and expert systems
- Reasoning, reactive, layered and hybrid agents
- Methods for designing agent-oriented analysis
- Speech, languages (KQML, FIPA) for agent communication
- Ontologies and description logistics for languages, i.e. XML
- Coalitions, co-operative and adversarial interaction in multi-agent decision making
- Voting, auctions, argumentation and negotiating and bargaining
- Criteria and exemplars for multi-agent system solutions

Module code	CSCK541	**NQF level**	Level 7
Credit value	15 credits	**Module duration**	8 weeks

SOFTWARE DEVELOPMENT IN PRACTICE

Module aims

This module aims to:

- Provide students with a comprehensive understanding of the theory and practice of modern software development.
- Provide students with hands-on experience of a current programming language.
- Provide students with a critical insight into the processes of interpreting and translating software procurer requirements into software realisation.
- Provide a systematic overview into the process of evaluating and testing software systems.
- Develop an appreciation of the legal, social, ethical and professional considerations pertinent to software development, and the risk factors involved.

Learning outcomes

Students will be able to:

- Develop a deep and systematic understanding of the process of modern software development from end user requirements to software delivery.
- Develop a systematic knowledge of the theory underpinning modern programming techniques and the practical application of these techniques.
- Develop a comprehensive insight into the process and practice of evaluating software implementations.
- Develop a deep and systematic understanding of the risk factors pertaining to software development, and the associated legal, ethical, social and professional issues to be taken into consideration.

Syllabus

- Software Engineering Principles
- Data and Operators
- Control Structures and Recursion
- Data structures
- Graphical user interfaces
- Files, streams and I/O techniques
- Advanced Data Structures
- Management of the Software Development Enterprise

Module code	CSCK542	**NQF level**	Level 7
Credit value	15 credits	**Module duration**	8 weeks

DATABASES AND INFORMATION SYSTEMS

Module aims

This module aims to:

- Provide a critical understanding of the design and realisation of database systems.
- Provide in-depth understanding of operation and usage of databases systems.
- Provide a comprehensive understanding of the administration and maintenance of database systems.
- Provide comprehensive insight into a range of database paradigms.

Learning outcomes

Students will be able to:

- Develop a deep and critical insight into database systems and computer information systems.
- Develop a comprehensive ability to implement a functioning database using current tools and structures, and employing current design practices.
- Demonstrate a critical understanding of database querying via analysis of results.
- Integrate appropriate security and backup in planning database maintenance and administration.

Syllabus

- Evolution and Fundamentals of Database Systems
- The Relational Model
- Analysis and Design of Database Systems
- Transaction Management
- Query Languages
- Database Connectivity
- Web Technology and DBs
- Alternative Database Paradigms

Module code	CSCK543	**NQF level**	Level 7
Credit value	15 credits	**Module duration**	8 weeks

NETWORKS & WEB TECHNOLOGY

Module aims

This module aims to:

- Develop a deep and systematic knowledge of the use of Web technologies to support business needs and objectives.
- Provide in-depth and critical understanding of current tools and techniques that support Web technologies.
- Develop high-level skills in development and maintenance of appropriate web-based systems.

Learning outcomes

Students will be able to:

- A deep and systematic understanding of the tools and techniques used to build Web applications.
- An ability to conduct in-depth analysis of the legal, social, ethical and professional issues relating to the practical deployment of Web technologies.
- An ability to create both static and dynamic web-based systems, using current tools and techniques, to support business needs and goals.
- An ability to critically analyse and evaluate Web applications in respect of usability and accessibility.

Syllabus

- Web Design
- Distributed Systems and Internet Protocols
- Markup Languages
- Dynamic Web Programming
- Server and Client-Side Scripting
- Scripting Languages
- The Semantic Web
- Advanced Web Technologies

Module code	CSCK508	**NQF level**	Level 7
Credit value	15 credits	**Module duration**	8 weeks

RESEARCH METHODS IN COMPUTER SCIENCE

Module aims

This module aims to:

- Provide a deep and systematic knowledge of the nature of strategic computing projects that harness recent development within the domain of computer science.
- Equip students with the ability to undertake independent research with a view to specifying a strategic IT project; including problem and solution definition, and the ability to compare and analyse competing solutions.
- Furnish an ability to manage, conduct and monitor strategic IT projects using a range of tools and techniques.
- Provide an in-depth knowledge and understanding of the information security issues related to the management, conducting and monitoring of IT projects, including the associated risk management.
- Highlight the Legal, Social, Ethical and Professional (LSEP) issues applicable to computing projects and the relevant codes of ethics and practices.
- Enhance and develop transferable skills in the context of the presentation and communication of technical material to a range of audiences.

Learning outcomes

Students will be able to:

- Investigate and define a problem in terms of recent innovations and the current technological state of the art; and in terms of end-user (customer) needs and cost drivers.
- Critically review current literature concerning key developments in a particular domain, and identify limitations and avenues with a view to further development and entrepreneurship.
- Define and evaluate a computing solution to a recognised problem taking into consideration technical constraints, risks and safety aspects; and the Legal, Social, Ethical and Professional Issues (LSEPI), including information security requirements.
- Manage the design, specification and implementation of a computing solution to a recognised problem using appropriate tools and practices.
- Critically evaluate a proposed computing solution to a recognised problem.

Syllabus

- Overview of research methods
- Legal, social, ethical and professional issues
- Literature review
- Research project specification
- Project management
- Project conduct
- Project evaluation
- Technical writing

Module code	CSCK700	**NQF level**	Level 7
Credit value	60 credits	**Module duration**	32 weeks

COMPUTER SCIENCE CAPSTONE PROJECT

Module aims

This module aims to:

- Equip students with the ability to plan and conduct an independent technical project over an extended period of time.
- Allow students to successfully complete a self-directed project culminating in a detailed written dissertation and video presentation.
- Provide an opportunity for students to reflect on and use tools and techniques acquired during the preceding taught part of the programme.
- Encourage students to consider and address the legal and ethical issues surrounding their project topic and relate these to the professional standards of the Chartered Institute for IT.

Learning outcomes

Students will be able to:

- Conduct independent research and development within the context of a computer science project.
- Produce detailed written documentation to a standard expected of a professional in the field of computer science.
- Develop a stand-alone artefact that meets the requirements identified and conforms to a design specification.
- Articulate the legal, social, ethical and professional issues surrounding an extended project, and follow relevant professional codes of practice.
- Communicate technical information clearly and succinctly to a broad, non-specialist audience.
- Evaluate project outcomes with reference to key research publications in the relevant field.

CYBER SECURITY

USEFUL INFORMATION

Learning and teaching methods

The mode of delivery is by online learning, facilitated by a Virtual Learning Environment (VLE). This mode of study enables students to pursue modules via home study while continuing in employment. Module delivery involves the establishment of a virtual classroom in which a relatively small group of students (usually 10-25) work under the direction of a faculty member. Module delivery proceeds via a series of eight one-week online sessions, each of which comprises an online lecture, supported by other eLearning activities, posted electronically to a public folder in the virtual classroom. The eLearning activities will include lecture casts, live seminar sessions, self assessment activities, reading materials and other multimedia resources. Communication within the virtual classroom is asynchronous, preserving the requirement that students are able to pursue the course in their own time, within the weekly time-frame of each seminar. An important element of the module provision is active learning through collaborative, cohort based, learning using discussion fora where the students engage in assessed discussions facilitated by the faculty member responsible for the module. This in turn encourages both confidence and global citizenship (given the international nature of the online student body).

Fees and funding

For current information on tuition fees and funding options, please ask our course consultants for more details. **+852 9545 5878**

Discounts and scholarships

For current information on discounts and scholarships, please ask our course consultants for more details. **+852 9545 5878**

Careers

As society grows increasingly dependent on the internet and technology, the demand for qualified cyber security professionals also grows. This programme is designed to develop technical skills with an immediate application in the workplace, and will position you to succeed within senior technical and managerial positions within the field.

Alongside the subject-specific knowledge you will gain during the programme, you will also develop professional skills such as communication, teamwork, critical thinking and research. These will enhance your CV, allowing you to improve your career prospects and access more senior roles.

READY TO APPLY?

Submit your application online

or contact our partner, Kaplan Higher Education Hong Kong, at

+852 2526 3686

info@kaplan.edu.hk

UNIVERSITY OF LIVERPOOL

The University of Liverpool works with partner, Kaplan Higher Education Hong Kong, to process applications and admissions.