MSc Cyber Security (Part-Time)

London Campus

Level of study: Postgraduate

Mode of study: Part-time

Duration: 2 years (15 weekends)

Response to Covid-19: Our focus is on providing a safe and welcoming learning environment and ensuring continued access to learning.

As a result of the coronavirus (Covid-19) pandemic and resulting social distancing requirements, we are intending to teach this course using a mix of on-campus and online learning activities. We continue to be guided by the Government to ensure our campus is Covid-secure. More information about our response to Covid-19 and FAQs are available here.

All information is accurate at the time of sharing. Courses starting in 2021 are offered as a mix of face to face and online learning. We continue to monitor government and local authority guidance in relation to Covid-19 and we are ready and able to flex accordingly to ensure the health and safety of our students and staff. Contact time is subject to increase or decrease in line with additional restrictions imposed by the government or the University in the interest of maintaining the health and safety and wellbeing of students, staff, and visitors, potentially to a full online offer, should further restrictions be deemed necessary in future. Our online activity will be delivered through Blackboard Ultra, enabling collaboration, connection and engagement with materials and people.

Overview

The issue of cyber security continues to be a major issue for both individuals and large corporations. It has been reported by the Cyber Security Breaches Survey 2018 that over four in ten businesses (43%) and two in ten charities (19%) experienced a cyber security breach or attack in the last 12 months.

For businesses, it is no longer a question of if a cyber-attack will occur but rather when, and as such, the demand for qualified IT security professionals has risen exponentially. Northumbria University s part-time MSc Cyber Security has been designed to give you the skills to meet this increased demand, including how to handle security incidents, identify new and existing threats, and determining methods to minimise them.

Key facts

- Part-time Masters degree based in Central London
- Continue working while you study with lectures delivered on 15 weekends spread throughout the 2-year course
- Build a critical understanding of governance and assurance, along with technology risk practices
- Learn how to handle security incidents, identify new and existing threats and methods to minimise them
- Provisional certification in Cyber Security from the NCSC (National Cyber Security Centre), placing us in an elite group of postgraduate providers to have achieved this standard
- Northumbria University is recognised as a Centre of Excellence in Cyber Security Research (ACEs-CSR) by the National Cyber Security Centre
- Undergraduate degree not essential for entry
- Also available as a full-time programme

Course information

Level of study: Postgraduate

Fee (UK/Home): £8,400

Entry requirements: 2:2 honours degree, or equivalent from a recognised university in a related subject Professional qualifications that are equivalent to an honours degree or work experience may also be acceptable .**Mode of study:** Part-time

Duration: 2 years (15 weekends)

Assessment methods: Coursework and exams

Scholarships or bursaries: unavailable

Student finance: available

Payment plan: available

Starts: Oct, Jan,

'22Apr,

'22Jul,

'22

About this course:

What will I study?

Incidents of cyber-crime have increased in the UK by 48% from 2013-14 according to PwC s Global State of Information Security Survey 2015, costing the UK up to £27bn a year. While their 2016 survey has reported a significant shift in the way organisations are taking action, including their willingness to invest in security.

Our MSc Cyber Security will teach you how to handle security incidents, identify new and existing threats and determine methods to minimise them. We will also provide in-depth coverage of the fundamental concepts, principles and technologies for network security. Going beyond just theoretical theory, you will be given a practical understanding of governance and assurance, along with technology risk practices.

Our MSc Cyber Security has been awarded provisional certification in Cyber Security from the NCSC (National Cyber Security Centre). This places us in an elite group of postgraduate providers which have achieved this standard.

This programme is also available full-time, or as MSc Cyber Security with Advanced Practice which includes an internship, consultancy project or research project.

How will I be taught and assessed?

Our MSc Cyber Security is designed to allow you to fit your studies around your working life and is assessed through modular assignments, exams and a final dissertation.

- All taught lectures are delivered across **15 weekends** spread throughout the 2-year programme. This is based on two 10 am-4 pm sessions over 15 weekends, you will also have an additional 6-hours of contact time through a **workshop.**
- You will also have 6-hours of **contact time with your tutor** as part of your final project, this can be on campus or online.
- You will also be expected to engage in **independent study, around 3-4 hours per week** on average over the 2 years. This will be supported by your module tutor and will consist of pre-class reading preparation, research, assessment preparation, development and writing as well as skills development and online tests and quizzes.
- **Assessment** includes a range of assessment methods including exams, assignments, presentations and group work.
- **Technology-enhanced** learning is embedded throughout the course to guide your preparation for seminars and independent research
- We offer extensive student support in and outside of the classroom with a dedicated student support team based in London.

Careers and further study

Cyber security has become an increasingly recurring issue for businesses, governments and the public. Recent hacks

include the US presidential election, Yahoo s 'biggest data breach in history and the continual release of information by WikiLeaks, the financial cost to business is estimated to be as high as $6 trillion by 2021. Given this, businesses and governments alike have significantly invested in their cyber security systems.

With all this investment, there are a plethora of career options following completion of this course, typical roles include:

- Threat management & forensics
- Risk analytics & management
- Policymakers & Strategists
- Operations & security management
- Engineering, Architecture & Design
- Chief Technology Officer

Related reading

From your Programme Leader, Hamid Jahankhani**:**

- Cyber Security Experts of the Future: The Role of Early Education on Cyber Security Awareness in the UK
- What is Cyber Crime and How Can Cyber Criminology Help Reduce Victimisation?
- Fighting Cyber-Crime

Cyber Security reading:

- Threats to Information Security 2019
- A Year On: Catching Up With A Cyber Security Alumnus
- The Year So Far in Cyber Security
- Meet our Cyber Security Lecturer: Dr John McCarthy
- The State of Cyber Security
- 11th International Conference on Global Security, Safety and Sustainability
- High Flying Jobs in Cyber Security
- The 11%; Where are the Women in Cyber Security?
- Popular Course: Cyber Security

Part-Time study:

- All You Need To Know About The Postgraduate Masters Degree Loans
- Q&A: What to Expect From Our Part-Time Masters Learning Advisor Service
- Your Step By Step Guide For Applying To Applying For a Part-Time Masters
- What Financing Options Are There Available For Part-Time Study?
- Investing In Employees: Corporate Sponsorship in Higher Education
- Infographic: Options For Financing Your Part-Time Masters

Enquire now

Entry requirements

Standard entry requirements

- Minimum 2:2 honours degree from a recognised university in a relevant subject (IT/Computer Science/related field) or
- Professional qualifications that are equivalent to an honours degree

Non-standard entry requirements

- Relevant qualifications and/or work experience will be taken into consideration where the applicant has the judged potential to benefit from the programme. Requests will be considered on an individual basis by the Programme Leader and relevant module tutors where appropriate.

If you do not have the required technical expertise from either previous study, professional qualifications or work experience, you may find the MSc Cyber Security Technology more suitable.

Please visit our entry requirements page for country-specific qualifications.

Enquire now

Modules

All modules on this course are core and 20 credits unless otherwise stated.

Information Governance and Security

In this module, you will learn about the information governance and cyber security principles that underpin the management of an organisation s information assets. You will critically analyse the key concepts, theories, standards and frameworks of information governance and security, including risk management.

It will enable you to evaluate an organisation s current approach to information governance and cyber security. You will have the expertise to advise on the design and implementation of an appropriate strategy for managing an organisation s information (ensuring all assets meet legal, regulatory, organisational and/or societal needs for information governance and

Network Security

The main objective of this module is to provide you with in-depth coverage of the fundamental concepts, principles and technologies for network security. This module will provide you with a theoretical and practical understanding on two important aspects related to security namely, data security and network security.

The module will cover a number of topics including cryptography, classical systems, IP protocol security, private and public-key cryptography, cryptographic protocols, hash functions, authentication, signature schemes, email and web security, viruses, and firewalls. The concepts introduced in lectures are reinforced with the help of extensive hands-on laboratory workshops.

You will also have the opportunity to develop practical networking skills by using Cisco IOS, a configuration of firewalls, switches and routers. You will also explore the wider impact of security via a consideration of related legal, ethical and social issues.

Wireless Networks and Security

This module is designed to be suitable for a variety of networking professional roles including those wishing to gain a deeper understanding of 802.11 protocols, security and enterprise deployment. You will study enterprise wireless deployment elements and methodologies. Basic RF characteristics for mobile systems. 802.11 protocol operation and technologies wireless security issues and attack vulnerabilities.

Information Assurance and Risk Management

This module will provide students with in-depth knowledge of the processes used in assuring the security of information during use, sharing, storage, transmission and disposal. It will cover the protection of the integrity, authenticity, availability and confidentiality of all classes of information. The module is designed to provide a comprehensive framework for ensuring the resilience of business activities during threats and disruptive events thus enabling the assessment of potential risks to the business which could result from disasters or emergency situations.

Ethical Hacking for Cyber Security

This module will enable learners to develop a deep understanding of both theoretical and practical aspects of Ethical Hacking. An essential part of a modern organisation s e-security includes rigorous testing and analysis to determine vulnerabilities. Carrying out such work requires a special skill set, which crosses, legal issues, psychology, computer networks along with a detailed understanding of system vulnerabilities and exploits. Additionally, you will be exposed to a collection of industry-standard hacking tools and will learn how to apply these in an ethical manner to determine system vulnerabilities.

Research Methods and Project Management

Throughout the world of science, engineering, technology and business, the ability to pursue research is seen as a requisite for continued career progression in the appropriate subject discipline. This module introduces students to the nature of research and the processes involved in carrying out research. General research approaches and methods for research will be introduced including literature searching, evaluation and reviewing. This general introduction will be followed by the inclusion of topics specifically designed to meet the requirements of the students programme of study.

MSc Computer Science and Digital Technologies Project (60 credits)

The aim of this module is to enable you to undertake a substantial academic research project at Masters Level and

present the results from this work in both written and oral forms. Your project itself will be a major piece of independent and original research centred at the forefront of your programme discipline within the wider sphere of the computer science and digital technologies field.

Enquire now

Fees and finance

Tuition fee 2021/22:

- £8,400

Tuition fee 2022/23:

- £9,075

Please note that your tuition fees do not include the cost of course books that you may choose to purchase, stationery, printing and photocopying, accommodation, living expenses, travel or any other extracurricular activities. As a Northumbria University London Campus student, you will have full access to our online digital library with over 400,000 e-books and 50,000 electronic journals.

The modules you will study do not require you to purchase additional textbooks although we recommend you allow an additional £200-250 for the duration of your studies should you choose to purchase any additional reading materials.

What's included in your tuition fees?

Your tuition fees cover far more than your time in class with our expert academics, it covers the cost of providing you with excellent services and student experience.

- Contact time in class – typically in lectures, seminars and tutorials
- Access to facilities, including computers, on-campus Wi-Fi, printers, vending machines, quiet study spaces
- The support of our Careers & Employment Service who help you to become more employable, secure placements and run workshops
- Academic support – our ACE Team run multiple sessions on academic writing, presenting, exam techniques throughout the semester, as well as 1-2-1 appointments and drop-in sessions
- Student support services such as our Ask4Help Service. Find out more about the services available to you on our Student Support page
- Access to online resources, including 24/ 7 Library with over 400,000 e-books and 50,000 electronic journals.

Payment plans

We offer an interest-free monthly payment plan available to all self-funded students after payment of your deposit.

Please note that self-funded students are required to pay a deposit of £2,450.

Government Loan for Masters study

If you are a UK/Home student, you may be eligible for a postgraduate loan of up to £10,000+ from the UK Government. Click here to find out more about the loan and whether you are eligible to receive it.

Payment plans and PGL

Early Application Discounts

Our Early Application Discount is awarded to you when you submit your application and holding deposit, before the deadlines specified on our **dates and fees page**. The discount is applied to your remaining fees after you pay your full deposit. This discount cannot be used in conjunction with any other offer – please contact us for more details on eligibility.

Enquire now

How to apply or find out more

How to find out more

Enquire now to find out more information about the course, studying with us, the application process, and to ask any other questions you may have.

Enquire now

How to apply

Once you re ready to apply, you can apply online to study the part-time MSc Cyber Security programme. This method allows you to upload your supporting documents at the time of application and automatically receive your student application number.

Apply online

We strongly recommend that you submit your application as early as possible to allow you to complete all of the preparations needed to study your programme. Please refer to the **Dates and Fees** page.

Supporting documents

For us to assess your application in a timely manner, it is important that you provide us with the following documents:

- Fully completed application form
- Personal email address must be included on the application form
- Transcripts and/or certificates (including a certified translation if not in English)
- Passport – copy of personal details page

- Proof of financial sponsorship if applicable
- Details of two referees
- Confirmation of immigration history including copies of previous and current visas if applicable
- An attached CV is desirable

You can check more information on <u>how to apply here</u>, including guidelines for the application forms.