

Module code: MOD005772		Version: 13 Date Amended: 16/Jul/2026	
-------------------------------	--	---	--

1. Module Title			
Cyber Crime Fundamentals			

2a. Module Leader			
Ronak Al-Haddad			

2b. School			
School of Computing and Information Sciences			

2c. Faculty			
Faculty of Science and Engineering			

3a. Level			
4			

3b. Module Type			
Standard (fine graded)			

4a. Credits			
15			

4b. Study Hours			
150			

5. Restrictions			
Type	Module Code	Module Name	Condition
Pre-requisites:	None		
Co-requisites:	None		
Exclusions:	None		
Courses to which this module is restricted:	None		

LEARNING, TEACHING AND ASSESSMENT INFORMATION

6a. Module Description

This module introduces the fundamental principles of security in IT and networked systems, combining theoretical foundations with practical application. You'll begin by exploring cybercrime, the contemporary threat landscape, and the impact of cyberattacks on individuals, organisations, and critical infrastructure. The module then examines security challenges affecting both host and networked environments, with particular emphasis on protecting data at rest, in transit, and during processing.

Core security concepts, including confidentiality, integrity, and availability, provide the framework for understanding how systems are designed to resist modern threats and vulnerabilities. You'll explore common attack vectors and defensive strategies, gaining insight into the technical, organisational, and human factors that influence cybersecurity.

Learning is supported through a combination of lectures and guided laboratory exercises, allowing you to apply theoretical concepts in realistic scenarios and develop practical skills in securing systems and networks. This blend of academic study and hands-on experience will help you understand how security controls are implemented and evaluated in professional environments.

By the end of the module, you'll have developed a solid foundation in cybersecurity principles and the ability to assess risks, identify vulnerabilities, and apply appropriate security measures to protect digital systems and information in an increasingly interconnected world.

6b. Outline Content

Security principles and threats
Introduction to Cyber crime (attacks, malware)
System Security
Network Security (Intrusion detection, network monitoring)
Basic Cryptography
Security in design and implementation
Professional IT and computing bodies
Applications of Security (DRM, online banking, smartcards)
Security Management and Human Aspects
Computer Forensics
Green computing

6c. Key Texts/Literature

The reading list to support this module is available at: <https://readinglists.aru.ac.uk/>

6d. Specialist Learning Resources

Students will have access to specialist computer labs equipped with security and networking monitoring tools, and online resources.

7. Learning Outcomes (threshold standards)		
No.	Type	On successful completion of this module the student will be expected to be able to:
1	Knowledge and Understanding	Identify the types of risk that may threaten an IT system.
2	Knowledge and Understanding	Explain mechanisms that may be used for achieving authentication and access control
3	Intellectual, practical, affective and transferrable skills	Recommend suitable means of protecting Internet systems and communications for different applications.
4	Intellectual, practical, affective and transferrable skills	Recognise the need to consider security in system design and implementation activities

8a. Module Occurrence to which this MDF Refers				
Year	Occurrence	Period	Location	Mode of Delivery
2026/7	ZZF	Template For Face To Face Learning Delivery		Face to Face

8b. Learning Activities for the above Module Occurrence			
Learning Activities	Hours	Learning Outcomes	Details of Duration, frequency and other comments
Lectures	12	1,2,4	Lecture 1 hour x 12 weeks
Other teacher managed learning	24	1,2,4	Practical 2 hour x 12 weeks
Student managed learning	114	1-4	Private study
TOTAL:	150		

9. Assessment for the above Module Occurrence

The assessment for some modules includes a presentation (see below for details on how this particular module is assessed). We recognise that presenting, especially to a large group, can cause significant anxiety or distress for some students. If this may affect you, please contact your Module Leader or the Disability and Neurodiversity Service as early as possible. We will work with you to consider appropriate reasonable adjustments. Depending on your individual needs, these might include, for example, presenting to a smaller group or presenting only to a member of academic staff.

Assessment No.	Assessment Method	Learning Outcomes	Weighting (%)	Fine Grade or Pass/Fail	Qualifying Mark (%)
010	Coursework	1-4	30 (%)	Fine Grade	30 (%)

In-class test (1 hour)

Assessment No.	Assessment Method	Learning Outcomes	Weighting (%)	Fine Grade or Pass/Fail	Qualifying Mark (%)
011	Coursework	1-4	70 (%)	Fine Grade	30 (%)

Report (1500 words)

In order to pass this module, students are required to achieve an overall mark of 40% (for modules at levels 3, 4, 5 and 6) or 50% (for modules at level 7*).

In addition, students are required to:

- (a) achieve the qualifying mark for each element of fine graded assessment as specified above
- (b) pass any pass/fail elements

[* the pass mark of 50% applies for all module occurrences from the academic year 2024/25 – see Section 3a of this MDF to check the level of the module and Section 8a of this MDF to check the academic year]