MODULE TITLE	**Information Security**	**CREDIT VALUE**	**15**
MODULE CODE	**ECMM442**	**MODULE CONVENER**	**Unknown**

DURATION: TERM	**1**	**2**	**3**
DURATION: WEEKS			

Number of Students Taking Module (anticipated)	**20**

DESCRIPTION - summary of the module content

DATA SCIENCE AND DATA SCIENCE WITH BUSINESS STUDENTS ONLY
The collection, storage and communication of data all create potential vulnerabilities to malicious exploitation. Security has become an important aspect of all kinds of data processing activity and therefore an important consideration for data scientists. In this module, you will gain a solid understanding of the main issues related to security in modern computer systems, networks and online environments. You will learn the foundations of computer security, techniques to secure complex digital systems, and gain practical skills in secure management of networked computer systems.
Pre-requisites: ECMM430 Fundamentals of Data Science.
Co-requisites: None.

AIMS - intentions of the module

As more aspects of human activity have been computerised, the security of digital systems against malicious or criminal exploitation has become ever more important. Trust is essential for commercial, financial, legal and governmental systems. Without robust information security, users cannot trust digital systems and the systems break down.
The aim of this module is to equip you with a range of knowledge and skills needed to make effective decisions in the context of information security. The module will cover the foundational concepts of computer security, including the nature of different kinds of malicious activity, technical features of digital systems that are vulnerable to exploitation (and how they can be protected), and modern technologies for enabling secure and trustworthy digital transactions.
The module will assume no knowledge beyond the mathematics and programming covered in pre-requisite ECMM430 Fundamentals of Data Science. The module will be taught in a one-week intensive block of lectures and associated practical work, together with individual self-study and coursework. Lectures will introduce the core topics, consolidated by practical exercises based on lecture material. Assessments will include assessed practical exercises and coursework.

INTENDED LEARNING OUTCOMES (ILOs) (see assessment section below for how ILOs will be assessed)

On successful completion of this module ***you should be able to***:
Module Specific Skills and Knowledge
1. Discuss the main concepts of information security.
2. Discuss the most common kinds of malicious activity relating to data and online transactions.
3. Demonstrate knowledge of techniques and methods for ensuring security in digital information systems.

Discipline Specific Skills and Knowledge
5. Understand the role of information security in online commercial, financial and other activities.
6. Use appropriate techniques to improve security of digital information.

Personal and Key Transferable / Employment Skills and Knowledge
7. Communicate ideas, techniques and results fluently using written means appropriate for the intended audience.
8. Communicate using notebooks and other digital media appropriate for a specialist audience.

SYLLABUS PLAN - summary of the structure and academic content of the module

Topics will include:
Malicious behaviours: hacking, malware, data theft, denial-of-service, online fraud
Secure storage
Data encryption and secure communication
Cybersecurity, network security and online privacy
Access control mechanisms
Firewalls and Intrusion detection
Malicious software and software security
Authentication and digital signatures
Blockchain and distributed ledgers

LEARNING AND TEACHING

LEARNING ACTIVITIES AND TEACHING METHODS (given in hours of study time)

Scheduled Learning & Teaching Activities	34.00	**Guided Independent Study**	116.00	**Placement / Study Abroad**	0.00

DETAILS OF LEARNING ACTIVITIES AND TEACHING METHODS

Category	Hours of study time	Description
Scheduled Learning & Teaching	16	Lectures
Scheduled Learning & Teaching	18	Practical Work
Guided independent study	50	Project Work
Guided independent study	66	Background Reading and Self-Study

ASSESSMENT

FORMATIVE ASSESSMENT - for feedback and development purposes; does not count towards module grade

Form of Assessment	Size of Assessment (e.g. duration/length)	ILOs Assessed	Feedback Method
Practical Exercises	18 hours	All	Oral

SUMMATIVE ASSESSMENT (% of credit)

Coursework	80	**Written Exams**	0	**Practical Exams**	20

DETAILS OF SUMMATIVE ASSESSMENT

Form of Assessment	% of Credit	Size of Assessment (e.g. duration/length)	ILOs Assessed	Feedback Method
Coursework (practical work and report)	80	Code notebook and 2000 word report	All	Written
Assessed practical exercises	20	1 hour	All	Written

DETAILS OF RE-ASSESSMENT (where required by referral or deferral)

Original Form of Assessment	Form of Re-assessment	ILOs Re-assessed	Time Scale for Re-assessment
Coursework (practical work and report)	Coursework (practical work and report)	All	Within 8 weeks
Assessed practical exercises	Assessed practical exercises		Within 8 weeks

RE-ASSESSMENT NOTES

Deferral – if you miss an assessment for certificated reasons judged acceptable by the Mitigation Committee, you will normally be either deferred in the assessment or an extension may be granted. The mark given for a re-assessment taken as a result of deferral will not be capped and will be treated as it would be if it were your first attempt at the assessment.
Referral – if you have failed the module overall (i.e. a final overall module mark of less than 50%) you will be required to re-take some or all parts of the assessment, as decided by the Module Convenor. The final mark given for a module where re-assessment was taken as a result of referral will be capped at 50%.

RESOURCES

INDICATIVE LEARNING RESOURCES - The following list is offered as an indication of the type & level of information that you are expected to consult. Further guidance will be provided by the Module Convener

Basic reading:

ELE: http://vle.exeter.ac.uk/

Web based and Electronic Resources:

Other Resources:

Reading list for this module:

Type	Author	Title	Edition	Publisher	Year	ISBN	Search
Set	Pfleeger, C. P., Pfleeger, S. L., Margulies, J	Security in Computing	5th	Prentice Hall	2015	978-0-13-408504-3	[Library]
Set	John R. Vacca	Computer and Information Security Handbook	2nd		2013		[Library]
Set	William Stallings, Lawrie Brown	Computer Security: Principles and Practice	3rd		2014		[Library]

CREDIT VALUE	15	**ECTS VALUE**	7.5
PRE-REQUISITE MODULES	ECMM430		
CO-REQUISITE MODULES			
NQF LEVEL (FHEQ)	7	**AVAILABLE AS DISTANCE LEARNING**	No
ORIGIN DATE	Tuesday 10 July 2018	**LAST REVISION DATE**	Wednesday 18 January 2023
KEY WORDS SEARCH	Information security, cybersecurity, online information		