MODULE SPECIFICATION PROFORMA

Module Code:	COM444

Module Title:	Introduction to Cyber Security

Level:	4	**Credit Value:**	20

Cost Centre(s):	GACP	JACS3 **code**: HECoS code:	I190 100376

Faculty:	Arts, Science and Technology	**Module Leader:**	Dr. Paul Comerford

Scheduled learning and teaching hours	36 hrs
Guided independent study	164 hrs
Placement	0 hrs
Module duration (total hours)	200 hrs

Programme(s) in which to be offered (not including exit awards)	Core	Option
BSc (Hons) Computer Science	☐	✓
BSc (Hons) Computing	☐	✓
BSc (Hons) Computer Networks and Security	☐	✓
BSc (Hons) Cyber Security	☐	✓
BSc (Hons) Computer Science (with Industrial Placement)	☐	✓
BSc (Hons) Computing (with Industrial Placement)	☐	✓
BSc (Hons) Computer Networks and Security (with Industrial Placement)	☐	✓
BSc (Hons) Cyber Security (with Industrial Placement)	☐	✓
Delivery as standalone or part of CPD package	☐	✓

Pre-requisites
None

Office use only
Initial approval: 28/11/2018 Version no:1
With effect from: 01/09/2019
Date and details of revision: Version no:

Module Aims
On this module students will learn the fundamental knowledge concerning computer security, basic cyber threats and the corresponding detection and defence techniques. Core security concepts, terminology, technologies and professional cyber security skills will be introduced via case studies and laboratory experiments.

Intended Learning Outcomes

Key skills for employability

KS1	Written, oral and media communication skills
KS2	Leadership, team working and networking skills
KS3	Opportunity, creativity and problem solving skills
KS4	Information technology skills and digital literacy
KS5	Information management skills
KS6	Research skills
KS7	Intercultural and sustainability skills
KS8	Career management skills
KS9	Learning to learn (managing personal and professional development, self-management)
KS10	Numeracy

At the end of this module, students will be able to		Key Skills	
1	Understand the basic concepts, terminology and technologies of cyber security.	KS3	
		KS5	
		KS6	
2	Develop an understanding of cyber threats and the corresponding detection and defence techniques.	KS2	
		KS5	
		KS6	
3	Consider the human factor in computer security.	KS6	
4	Acquire an understanding of different types and use of available security software.	KS3-5	
5	Reflect on their learning and development within the context of cyber security.	KS1-5	

Transferable skills and other attributes

Derogations

None

Assessment:

Indicative Assessment Tasks:

Students are assessed by three compulsory assessments
The first assessment is a 1.5-hour class test aimed at the student's capability to understand material covered throughout the module.

The second compulsory assessment is an assignment based on the successful completion of a series of workshop tasks or on a given case study scenario. It will allow students to demonstrate their awareness of the contexts in the detection and prevention of cyber attacks. Students will produce a report (about 2000 words in total) detailing their findings of the investigation.
The third compulsory assessment, 2-hour practical test, is designed to assess the understanding of fundamental concepts and their practical application.

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)	Duration (if exam)	Word count (or equivalent if appropriate)
1	1,5	In-class test	20	1.5 hours	
2	1,3,5	Case Study	50		2000
3	1-4	Practical	30	2 hours	

Learning and Teaching Strategies:

Students will develop understanding and practical investigative skills based on weekly lectures, tutorials and supervised workshops. The teaching sessions will utilise examples/case studies as a platform for understanding security threats and how to counter them. The workshops, in particular, are provided to support students in gaining practical experience in computer security, within a dedicated laboratory.
Appropriate blended learning approaches and technologies, such as, the University's VLE and computer security tools, will be used to facilitate and support student learning, in particular, to:

- deliver content;
- encourage active learning;
- provide formative and summative assessments, and prompt feedback;
- enhance student engagement and learning experience.

Students will be expected and encouraged to produce reflective commentaries on the learning activities and tasks that they carry out to complete their work.

Syllabus outline:

Introduction to cyberspace and cyber security: computer security, web security, operating system security, wireless/network security, mobile security, programming security.
Concepts and terminology of cyber security: basics of encryption and cryptography, virtual platform, cloud, protocols, hacking, malware, virus, botnets, pentest, information security practice/standards.

Basic coverage of security software: anti-virus software, packet sniffers, anti-spyware, intrusion detection/protection software, digital forensics software, pentest software.

Introductory overview of network security: types of networks, network protocols, network security and protection, VPNs, firewall configuration/maintenance, network intrusion and detection systems.

The human factor in security: authorisation mechanisms, usability issues, risk analysis and control, cyber-ethics, cyber bullying, social media attacks.

Indicative Bibliography:

Essential reading

Gollmann, D. (2011), *Computer Security.* 3rd ed. John Wiley.

Goodrich, M. and Tamassia, R. (2013), *Introduction to Computer Security*. Harlow: Pearson.

Easttom, W. (2016), *Computer Security Fundamentals.* 3rd ed. Harlow: Pearson.

Other indicative reading

Gee, G. (2014), *Cyber Security Principles*. San Ramon: CA: Paper Street Publishing.

Department for Business, Innovation and Skills. (2014). CyberSecurity. Available: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview