COURSE SPECIFICATION DOCUMENT

Academic Department:	Science, Innovation & Technology
Programme:	Computer Science
***FHEQ* Level:**	5
Course Title:	Cyber Security
Course Code:	COMP 5102
Student Engagement Hours:	160
Timetabled Hours:	45
Guided Learning Hours:	15
Independent Learning Hours:	100
Credits:	16 UK CATS credits 8 ECTS credits 4 US credits

Course Description:

This course considers online security and protection. Students will learn how to identify threats and take steps to reduce vulnerabilities. The course will frame digital safety in the context of the Web, introducing concepts like malware, viruses, Trojans, network security, cryptography, identity theft and risk management, and will outline contemporary security strategies being developed. This class would be of particular interest to business, communications and international relations students. It is highly recommended that students have access to the use of a laptop and a smartphone for the duration of the course.

Prerequisites:

40 credits

Aims and Objectives:

The primary aim of this course is to familiarise students with online security terminology and protection strategies for business or home. It will focus on understanding and using cryptography terminology and its applications. Students will be able to understand the range of malware types for example Adware, Spyware, Trojan horse, Ransom ware and learn the skills to for preventing malware attacks. They will have guidance in contextualising this through appropriate examples and case studies. Alongside using a range of software, students will be required to maintain a reflective technical journal that can act as a reference point for problem solving and protection from online threats in the future.

Programme Outcomes:

L5 AI, II, BI, II, CI, II, DI, II

A detailed list of the programme outcomes is found in the Programme Specification. This is maintained by Registry and located at: https://www.richmond.ac.uk/programme-and-course-specifications/

Learning Outcomes:

By the end of this course, successful students should be able to:

- Demonstrate an ability to identify, analyse and evaluate a range of cyber security strategy and digital information assets.
- Demonstrate an ability to identify main malware types, cryptography terminology and be aware of alternate authentication methods.
- Demonstrate understanding of firewalls, networks and recoveries from security failures.
- Assess security needs, design and break security systems.
- Engage in self-directed research to problem solve technical issues to produce innovative solutions.

Indicative Content:

- Computer Security and Terminology
- Threats
- Malware
- Authentication
- Assessing security needs
- Case Studies
- Current and future security trends

Assessment:

This course conforms to the University Assessment Norms approved at Academic Board and found at https://www.richmond.ac.uk/university-policies/

Teaching Methodology:

This course will be delivered face to face through a combination of lectures and interactive sessions. In addition to classroom activities, there are guided learning elements that are tutor led and arranged through Blackboard. These activities can be asynchronous online sessions, flipped classrooms, set readings with discussion boards or set guest lectures for example. Set activities are monitored by the instructor to ascertain student engagement. Students are encouraged to prepare for class and to play an active part, to raise questions, following-up ideas and interact with a wide range of provided material.

Indicative Text(s):

Cerra, A. (2019) *The cybersecurity playbook: how every leader and employee can contribute to a culture of security*. Wiley.

Ouaissa, M. and Ouaissa, M. (2024) *Offensive and Defensive Cyber Security Strategies: Fundamentals, Theory and Practices.* CRC Press

Reuvid, J. (2019) *Managing Cybersecurity Risk; Book 3.* Legend Business publishing.

Wilson, D. (2021) *Cybersecurity.* MIT Press.

Websites

The national Cyber Security Centre. Available at: https://www.ncsc.gov.uk/ (Accessed: November 2024).

Reuters news agency. Available at: https://www.reuters.com/news/archive/cybersecurity (Accessed: November 2024).

Wired. Available at: https://www.wired.com/tag/cybersecurity/ (Accessed: November 2024).

Digital Health. Available at: https://www.digitalhealth.net/2019/02/cyber-security-news-round-up-5/ (Accessed: November 2024).

See syllabus for complete reading list.

Change Log for this CSD:

Nature of Change	Date Approved & Approval Body (School or AB)	Change Actioned by Registry Services
First Edition	Nov 2024	