University of Essex

Online

Module code	LCYS_PCOM7E	NQF level	7
Credit value	20	Study duration	12 weeks

Launching into Cyber Security

Module description

The module will explore and investigate the fundamental theories and practices of computing and then gradually explore the trends and current developments in the field of cyber security. The module introduces the historical, architectural and practical perspectives of the computer science discipline, also enables the learners to get engage, experience and envision the current,as well as the future,developments in cyber security. This involves equipping students with the practical skills required to be able to analyse an information system problem, design and implement a solution using suitable programming languages. The module is designed not only to equip the students with an understanding of concepts and knowledge, but also to make the learners be aware of the ethical and professional responsibilities of the cyber security professional.

This module aims to:

- Instil amongst students:
  - an understanding of the professional roles, skillset, ethical responsibilities of cyber security professionals
  - an understanding of the relevant computing architectures, practices, applications and standards
  - an understanding of the core concepts in cyber security such as cryptography, penetration testing and ethical hacking
  - an understanding of programming concepts and practices necessary for facilitating security-based solutions to identified problems.
  - a development of competent skills in applying algorithm and programming practices, gaining individual confidence in developing computer programs.
  - the ability to implement a secured information system using the principles and concepts of object-oriented approaches to solve a given problem, such as information system design and web development.
  - an ethos of professional development highlighting major ethical-social-corporate responsibilities underpinning the concepts of threats, securities and global impacts prevailing the recent technological innovations and future applications

Learning outcomes

On completion of this module, students will be able to:

- Identify and explain the architecture, structure and functionality of basic components of a computer system, considering cyber security issues
- Evaluate critically implications of the key vulnerabilities and threats of software and network security and approaches to mitigate these issues
- Appraise critically and apply the concepts and principles of secured object-oriented programming and design to facilitate business security-based decisions
- Evaluate critically the solutions developed to solve/mitigate these security issues

Syllabus

- Cyber security professional roles, skillset, ethical and legal responsibilities, and resources available
- Introduction to computing infrastructure and operating systems
- Threats and security in software and network systems
- Cyber security concepts, including Cryptography, Penetration testing and Ethical hacking
- Fields and emerging trends in cyber security, including Cloud Computing Technologies and Internet of Things
- Object-oriented Analysis, Design and Programming techniques for secured systems
- Database design and implementation
- Secure web development

Learning and teaching methods

The module will be delivered through the provision of specified reading materials on the virtual learning platform, which shall be supported by specified online discussion forums and lecturecasts. The flexible and participative approach of the module will develop a collaborative research inquiry in the advancement of computing, enabling them to accelerate in their chosen career.

Students will demonstrate their ability and strengths through evidence and reflections by maintaining an e-portfolio. The e-portfolio will also act as a means for assessment on evidence of personal growth and CPD.

Synchronous sessions will give students the opportunity to interact with fellow students and for tutor contact. The sessions will include live coding sessions to help students contextualise their knowledge. These synchronous sessions will be recorded in order to ensure that all students can access the material in their own time.

At pre-arranged days and agreed times during the module (usually weekly, prior to a synchronous session), the module tutor will be available for a drop in telephone or preparatory learning liaison session. This is to give students the opportunity to ask specific and general questions relating to the week's learning opportunities and enable them to contextualise their learning.

For team activities in this module, students will be grouped according to time zones to ensure team members can communicate easily with each other. Details on the process for team activities and peer assessment will be made available to students at the outset of the module.

Description of unit of assessment	Length/Duration	Submission date	Weighting
Collaborative discussion summaries	600 words	Units 3 and 8	20%
Essay	2,000 words	Unit 9	40%
Individual implementation of programming code and written commentary	1,500 words equivalent	Unit 12	40%