INFO 2007 CYBER CRIME AND SOCIAL ENGINEERING (BLOCK)

Credit Points 10

Legacy Code 500075

Coordinator Mia Hatzistergos (https://directory.westernsydney.edu.au/search/name/Mia Hatzistergos/)

Description This subject focuses on both the theory and application of cyber crime and cybersecurity. More specifically, it focuses on the intersection between human behaviour, cyber crime, and cyber security with topics ranging from social engineering to organisational security infrastructure. It asks - What outcomes do cyber criminals seek? How can you protect yourself and your business from cyber crime? What methods do cyber criminals typically use to gain their desired outcomes? In this subject, cyber crime and cyber security is covered from both a theory-based and applied understanding of how to reduce the likelihood of or harm caused by cyber crime.

School Social Sciences

Discipline Security Science

Student Contribution Band HECS Band 2 10cp

Check your fees via the Fees (https://www.westernsydney.edu.au/currentstudents/current_students/fees/) page.

Level Undergraduate Level 2 subject

Pre-requisite(s) INFS 1013

Equivalent Subjects INFO 2001 - Cyber Crime and Cyber Safety
INFO 2004 - Cyber Crime and Social Engineering

Restrictions

Students must be enrolled in program 7179 - Undergraduate Certificate in Cybersecurity, Cybercrime and Behaviour.

Assumed Knowledge

A basic understanding of computer systems and network structures. This knowledge is gained as the student progresses through their first Block in the program with a start-year intake; or from the completion of two Blocks in the program in the case of a mid-year intake. A basic understanding of core theories related to social and cognitive psychology is desirable but not essential.

Learning Outcomes

On successful completion of this subject, students should be able to:

1. Define cyber crime and cyber safety by its related theories, terms and methods of investigation.
2. Compare and contrast cyber criminal practices with standard criminal practices.
3. Describe effective interventions to reduce susceptibility and risk from cyber attacks on an individual or organisation.
4. Evaluate the quality of organisational preparedness for cyber crime and susceptibility to different cyber criminal tools.
5. Develop an approach to identifying and assessing weak points in organisational defences.

Subject Content

Introduction and History of Cyber Crime
Online Safety ? applied and theoretical perspectives
Cyber criminals and cyber crime practices
Vulnerability to cyber crime and social engineering attacks
Protection from cyber crime and social engineering attacks on individuals and organisations

Assessment

The following table summarises the standard assessment tasks for this subject. Please note this is a guide only. Assessment tasks are regularly updated, where there is a difference your Learning Guide takes precedence.

Type	Length	Percent	Threshold	Individual/ Group Task
Quiz	10 Questions/20 Minutes, 10 Questions + 5 Short answer/40 Minutes, 20 Questions + 5 scenario Questions	35	N	Individual
Case Study	1000 Words	35	N	Individual
Presentation	20 Minutes (5-7 minutes per student), 500 Words	30	N	Group

Teaching Periods

Block C Session (2024)

Online

Online

Subject Contact Mia Hatzistergos (https://directory.westernsydney.edu.au/search/name/Mia Hatzistergos/)

View timetable (https://classregistration.westernsydney.edu.au/even/timetable/?subject_code=INFO2007_24-BC_ON_2#subjects)

Block F Session (2024)

Online

Online

Subject Contact Rachel Renwick (https://directory.westernsydney.edu.au/search/name/Rachel Renwick/)

View timetable (https://classregistration.westernsydney.edu.au/even/timetable/?subject_code=INFO2007_24-BF_ON_2#subjects)