

INFO 2004 CYBER CRIME AND SOCIAL ENGINEERING

Credit Points 10

Legacy Code 102700

Coordinator Farnaz Farid ([https://directory.westernsydney.edu.au/search/name/Farnaz Farid/](https://directory.westernsydney.edu.au/search/name/Farnaz%20Farid/))

Description This unit 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 unit, 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 HECS Band contribution amount via the Fees (https://www.westernsydney.edu.au/currentstudents/current_students/fees/) page.

Level Undergraduate Level 2 subject

Pre-requisite(s) INFS 1002

Equivalent Subjects INFO 2001 Cyber Crime and Cyber Safety

Assumed Knowledge

A basic understanding of computer systems and network structures. This knowledge is gained as the student progresses through their first semester in the program with a start-year intake; or from the completion of two semesters 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.

Item	Length	Percent	Threshold	Individual/Group Task
Quiz	10 X 5 MCQ each	10	N	Individual
Case Study	1,000 words	35	N	Individual
Presentation	20 minutes	15	N	Group
Final Exam	2 hours	40	N	Individual

Prescribed Texts

- Hadnagy, C. (2010). Social engineering: The art of human hacking. John Wiley & Sons

Teaching Periods

WSU Online TRI-2

Wsu Online

Online

Subject Contact Natasha Daraio ([https://directory.westernsydney.edu.au/search/name/Natasha Daraio/](https://directory.westernsydney.edu.au/search/name/Natasha%20Daraio/))

View timetable (https://classregistration.westernsydney.edu.au/even/timetable/?subject_code=INFO2004_22-OT2_OW_O#subjects)

Spring

Parramatta - Victoria Rd

Day

Subject Contact Farnaz Farid ([https://directory.westernsydney.edu.au/search/name/Farnaz Farid/](https://directory.westernsydney.edu.au/search/name/Farnaz%20Farid/))

View timetable (https://classregistration.westernsydney.edu.au/even/timetable/?subject_code=INFO2004_22-SPR_PS_D#subjects)