COURSE OUTLINE

SEC708 Psychology of Cybercrime

School: School of Science, Technology and Engineering

2026 | Semester 1

Online	ONLINE	You can do this course without coming onto campus, unless your program has specified a mandatory onsite requirement.

Please go to unisc.edu.au for up to date information on the teaching sessions and campuses where this course is usually offered.

1. What is this course about?

1.1. Description

In this online course you will be introduced to the theories that explain how scammers, identity thieves and cybercriminals achieve their deception. You will also develop your knowledge of human behaviours, cognitive influences, and the psychosomatic impacts for victims of these crimes. Learn how to build prevention and awareness frameworks and campaigns, including underpinning performance measures which address consumer, institutional and broader response system requirements. You will also examine deceptive conduct and its behavioural levers and dependencies.

1.2. How will this course be delivered?

ACTIVITY	HOURS	BEGINNING WEEK	FREQUENCY
ONLINE			
Online	2hrs	Week 1	13 times

1.3. Course Topics

1. Cyberpsychology
2. History of cybercrime and scams.
3. Online scams – definition and types.
4. Economics of cybercrime
5. Summary of the most revalent and costly cybercrime scams
6. Modern scams and the broader history of deception?
7. Criminological theories to understand cybercrime-related deviance
8. The impact of anonymising technologies and the online environment on human behaviours
9. Scammers' methodologies
10. Victim Psychology
11. Common causes of identity theft and the risks it presents to individuals and organisations
12. How identity theft is enabled, prevented, detected and responded to by organisations in different sectors
13. The role of government and particularly law enforcement in the cybercrime and identity theft response landscape
14. The responsibilities of organisations impacted by identity fraud and identity theft
15. Changes to improve Australia's resilience to identity fraud and to improve organisations' responses
16. Immediate and ongoing financial impacts of identity compromise and identity theft
17. Immediate and ongoing emotional and psychological impacts?
18. The typical response journey for a victim of identity compromise or identity theft
19. Individuals' experiences when seeking assistance from organisations such as financial institutions and law enforcement
20. Organisational support to improve their engagements with victims of identity compromise and identity theft, and where can they look to improve
21. Scam methodologies
22. Prevention and awareness strategies, including public awareness campaigns.
23. How theories from criminology can assist our understanding of cybercrime prevention and awareness.
24. How to effect behavioural change among online users.
25. The measures organisations and service providers can take to minimise victimisation.
26. How legal measures can reduce victimisation.
27. Cyber bulliying
28. Cyber stalking
29. The role of the Internet in facilitating radicalisation.
30. Overt and covert uses of the Internet by extremist and terrorist organisations.
31. Radicalisation mechanisms.
32. Group identity and psychology

2. What level is this course?

700 Level (Specialised)

Demonstrating a specialised body of knowledge and set of skills for professional practice or further learning. Advanced application of knowledge and skills in unfamiliar contexts.

3. What is the unit value of this course?

12 units

4. How does this course contribute to my learning?

COURSE LEARNING OUTCOMES		GRADUATE QUALITIES
On successful completion of this course, you should be able to...		Completing these tasks successfully will contribute to you becoming...
1	Critique key components and processes involved in historical through to contemporary forms of cybercrime offending.	Creative and critical thinker
2	Apply behavioural and criminological frameworks that explain cybercrime offending.	Empowered
3	Identify attributes of cybercrime victimisation and the response system.	Knowledgeable
4	Use analytical skills to construct cybercrime profiles, prevention and awareness models.	Empowered
5	Explain key ethical and practice challenges associated with cybercrime prevention and response from a multi-stakeholder perspective.	Ethical

5. Am I eligible to enrol in this course?

Refer to the UniSC Glossary of terms for definitions of “pre-requisites, co-requisites and anti-requisites”.

5.1. Pre-requisites

Not applicable

5.2. Co-requisites

Not applicable

5.3. Anti-requisites

Not applicable

5.4. Specific assumed prior knowledge and skills (where applicable)

Not applicable

5.5. Microcredential Information

Not applicable

6. How am I going to be assessed?

6.1. Grading Scale

Standard Grading (GRD)

High Distinction (HD), Distinction (DN), Credit (CR), Pass (PS), Fail (FL).

6.2. Details of early feedback on progress

Using marking rubrics, students will participate in continuous peer and self-assessment tasks. You will receive weekly formative feedback in tutorials from week 3 to assist with developing your assessment skills and completing assessment tasks. Tutorial review questions will be uploaded weekly and the accommodation of online chat forums will assist in developing peer-led learning experiences.

6.3. Assessment tasks

DELIVERY MODE	TASK NO.	ASSESSMENT PRODUCT	INDIVIDUAL OR GROUP	WEIGHTING %	WHAT IS THE DURATION / LENGTH?	WHEN SHOULD I SUBMIT?	WHERE SHOULD I SUBMIT IT?
All	1	Oral and Written Piece	Group	20%	10 minutes per presentation per week plus feedback	Week 4	Online Assignment Submission with plagiarism check
All	2	Activity Participation	Individual	30%	2000 words	Week 9	Online Assignment Submission with plagiarism check
All	3a	Practical / Laboratory Skills	Group	10%	2 hours	Refer to Format	In Class
All	3b	Report	Individual	40%	3000 words	Week 13	Online Assignment Submission with plagiarism check

All - Assessment Task 1: Case Study Development

GOAL:	The goal of this assessment is to provide opportunities for you to work in a group of between two and four students to learn and apply behavioural and criminological frameworks to a real-life case.
PRODUCT:	Oral and Written Piece
AUTHORSHIP STATEMENT:	
FORMAT:	Students are required to present online to their peers within their tutorial using visual aids accessible to their audience. They will support the presentation with a written report on the case for submission by Friday of Week 4. Groups will be formed, and case studies assigned, in your Week 2 tutorial. Working in tutorials and in an online wiki, each group will develop their presentation through a synthesis of their case and the application of relevant theoretical frameworks that assist to determine the motivation of offending, the impact of offending from a multi-stakeholder perspective, anticipated intervention responses, and consequences. Students must submit an assignment of no more than 1,500 words. In tutorial during weeks 3 to 4; Final report submission due Friday, Week 4.
CRITERIA:	

No.		Learning Outcome assessed
1	Critique of components and processes	
2	Application of frameworks	
3	Identification of cybercrime attributes	
4	Analysis cybercrime profiles and models	
5	Communication	
6	Assessment criteria are mapped to the course learning outcomes.	1 2 3 4 5

GENERIC SKILLS:	

All - Assessment Task 2: Written Behavioural Profile

GOAL:	The goal of this assessment task is to allow you to synthesise and apply your knowledge and skills developed through assessment 1 to construct a written case profile report on a selected case study. In your report, you will be required to demonstrate your ability to research, analyse and discuss the key processes undertaken
PRODUCT:	Activity Participation
AUTHORSHIP STATEMENT:	
FORMAT:	This task will require you to use basic assessment and case formulation skills to write a formal cybercrime behavioural profile report on an assigned case study. You are required to draw on literature to support your methods and formulation
CRITERIA:	

No.		Learning Outcome assessed
1	Critique of components and processes	
2	Development of behavioural profile	
3	Identification of cybercrime victimisation and response	
4	Explanation of ethical practice and challenges	
5	Communication skills	

GENERIC SKILLS:	

All - Assessment Task 3a: Lab Experiment Plan, Design and Execution

GOAL:	The purpose of this assessment task is to plan, develop and test a phishing simulation for a workplace. Students are required to document their planned approached, performance metrics, and anticipated responses. In groups of between four and six students, teams are to perform the simulation on themselves using a course provided software simulation and capture results.
PRODUCT:	Practical / Laboratory Skills
AUTHORSHIP STATEMENT:	
FORMAT:	This task will take the form of an in-class experiment where students design their own phishing detection tests and carry these out in their assessment groups (the test audience). Due: weeks 11 and 12.
CRITERIA:	

No.		Learning Outcome assessed
1	Development of cybercrime phishing	
2	Analysis of victim responses	
3	Explanation of ethical practice and challenges	
4	Critique of components of contemporary forms of cybercrime	
5	Communication skills	

GENERIC SKILLS:	

All - Assessment Task 3b: Report

GOAL:	The purpose of this assessment is to provide an individual report on the undertaking of the phishing experiment and considerations for improving phishing prevention and awareness in the simulated environment (the workplace).
PRODUCT:	Report
AUTHORSHIP STATEMENT:	
FORMAT:	The Report shall be no more than 3000 words and be targeted at an executive audience interested in building the resilience to phishing-born cyber attacks in the workplace. Suggested report outlines will be covered in class and will include an Executive Summary and any relevant appendices as part of the word count limit
CRITERIA:	

No.		Learning Outcome assessed
1	The appropriateness of its content for an Executive (C-suite) audience	
2	The experimental design, its reasoning, delivery and lessons observed	
3	The synthesis of the results and its applicability to the organisations environment (people, processes and technology).	
4	Consideration of the ethical challenges	
5	Applicability of prevention and awareness strategies and how they relate to your knowledge of relevant theoretical frameworks	
6	The quality and appropriateness of the recommendations made for the organisation in building cyber resilience and a security culture	

GENERIC SKILLS:	

7. Directed study hours

A 12-unit course will have total of 150 learning hours which will include directed study hours (including online if required), self-directed learning and completion of assessable tasks. Student workload is calculated at 12.5 learning hours per one unit.

8. What resources do I need to undertake this course?

Please note: Course information, including specific information of recommended readings, learning activities, resources, weekly readings, etc. are available on the course Canvas site– Please log in as soon as possible.

8.1. Prescribed text(s) or course reader

You need regular access to the resource(s) below. Many texts are available as ebooks through the Library at no additional cost.

REQUIRED?	AUTHOR	YEAR	TITLE	EDITION	PUBLISHER
Required	Kirwan, G. and Power, A	2013	Cybercrime: The Psychology of Online Offenders	n/a	Cambridge University Press

8.2. Specific requirements

This is an online course and will require access to a computer and the internet for at least 12 hours per week

9. How are risks managed in this course?

Health and safety risks for this course have been assessed as low. It is your responsibility to review course material, search online, discuss with lecturers and peers and understand the health and safety risks associated with your specific course of study and to familiarise yourself with the University's general health and safety principles by reviewing the online induction training for students, and following the instructions of the University staff.

10. What administrative information is relevant to this course?

10.1. Assessment: Academic Integrity

Academic integrity is the ethical standard of university participation. It ensures that students graduate as a result of proving they are competent in their discipline. This is integral in maintaining the value of academic qualifications. Each industry has expectations and standards of the skills and knowledge within that discipline and these are reflected in assessment.

Academic integrity means that you do not engage in any activity that is considered to be academic fraud; including plagiarism, collusion or outsourcing any part of any assessment item to any other person. You are expected to be honest and ethical by completing all work yourself and indicating in your work which ideas and information were developed by you and which were taken from others. You cannot provide your assessment work to others. You are also expected to provide evidence of wide and critical reading, usually by using appropriate academic references.

In order to minimise incidents of academic fraud, this course may require that some of its assessment tasks, when submitted to Canvas, are electronically checked through Turnitin. This software allows for text comparisons to be made between your submitted assessment item and all other work to which Turnitin has access.

10.2. Assessment: Additional Requirements

Eligibility for Supplementary Assessment Your eligibility for supplementary assessment in a course is dependent of the following conditions applying: The final mark is in the percentage range 47% to 49.4% The course is graded using the Standard Grading scale You have not failed an assessment task in the course due to academic misconduct

10.3. Assessment: Submission penalties

Late submission of assessment tasks may be penalised at the following maximum rate: - 5% (of the assessment task's identified value) per day for the first two days from the date identified as the due date for the assessment task. - 10% (of the assessment task's identified value) for the third day - 20% (of the assessment task's identified value) for the fourth day and subsequent days up to and including seven days from the date identified as the due date for the assessment task. - A result of zero is awarded for an assessment task submitted after seven days from the date identified as the due date for the assessment task. Weekdays and weekends are included in the calculation of days late. To request an extension you must contact your course coordinator to negotiate an outcome.

10.4. Links to relevant University policy and procedures

For more information on Academic Learning & Teaching categories including:

- Assessment: Courses and Coursework Programs
- Review of Assessment and Final Grades
- Supplementary Assessment
- Central Examinations
- Deferred Examinations
- Student Conduct
- Students with a Disability

For more information, visit https://www.usc.edu.au/explore/policies-and-procedures#academic-learning-and-teaching

10.5. Student Charter

UniSC is committed to excellence in teaching, research and engagement in an environment that is inclusive, inspiring, safe and respectful. The Student Charter sets out what students can expect from the University, and what in turn is expected of students, to achieve these outcomes.

10.6. General Enquiries

In person:

- **UniSC Sunshine Coast** - Student Central, Ground Floor, Building C, 90 Sippy Downs Drive, Sippy Downs
- **UniSC Moreton Bay** - Service Centre, Ground Floor, Foundation Building, Gympie Road, Petrie
- **UniSC SouthBank** - Student Central, Building A4 (SW1), 52 Merivale Street, South Brisbane
- **UniSC Gympie** - Student Central, 71 Cartwright Road, Gympie
- **UniSC Fraser Coast** - Student Central, Student Central, Building A, 161 Old Maryborough Rd, Hervey Bay
- **UniSC Caboolture** - Student Central, Level 1 Building J, Cnr Manley and Tallon Street, Caboolture

Tel: +61 7 5430 2890

Email: studentcentral@usc.edu.au