

CRM310 Introduction to Cyber Crime

School: School of Law and Society

2026 | Trimester 1

UniSC Sunshine Coast
UniSC Moreton Bay

**BLENDED
LEARNING**

Most of your course is on campus but you may be able to do some components of this course online.

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

This course is set up as an introductory course in cyber crime for criminology and related students.

In this course you will learn about types of cybercrime and cybercrime trends. We will cover topics such as defining cybercrime, the prevalence and impact of different types of online crimes, characteristics of offenders and victims, and how criminological theories can be used to understand how and why cybercrime occurs. This course also investigates responses and prevention of cybercrime and the challenges posed by investigating online crimes.

1.2. How will this course be delivered?

ACTIVITY	HOURS	BEGINNING WEEK	FREQUENCY
BLENDED LEARNING			
Learning materials – Online learning materials for 12 weeks (or equivalent).	1hr	Week 1	12 times
Tutorial/Workshop 1 – On campus tutorials	2hrs	Week 1	10 times
ONLINE			
Learning materials – Online learning materials for 12 weeks (or equivalent).	1hr	Week 1	12 times
Tutorial/Workshop 1 – Online tutorials	2hrs	Week 1	10 times

1.3. Course Topics

This course is designed for students without any background in Information Technology (IT). Therefore, it is not expected that students have specialised knowledge about IT systems. All topics contain mature content. This course covers the following topics

- Introduction to cybercrime,
- Offender and victims of cyber crime,
- Impacts of cybercrime,
- Cyber crime types and methodologies,
- Theories of cybercrime,
- Online terrorism,
- The dark net,
- Enforcement and investigation,
- Cybersecurity and prevention.

1.4. Mature Content

Drug Use, Sex/Sexual references, Violence, Coarse Language, Adult themes

2. What level is this course?

300 Level (Graduate)

Demonstrating coherence and breadth or depth of knowledge and skills. Independent application of knowledge and skills in unfamiliar contexts. Meeting professional requirements and AQF descriptors for the degree. May require pre-requisites where discipline specific introductory or developing knowledge or skills is necessary. Normally undertaken in the third or fourth full-time study year of an undergraduate program.

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 Develop and support their own arguments using evidence-based research and critical analysis	Creative and critical thinker Empowered
2 Have an understanding of cybercrime trends, types, impacts, and methods used to undertake cyber dependent and cyber enabled offences.	Empowered
3 Understand and apply criminological theories to cybercrime	Knowledgeable Creative and critical thinker
4 Analysing and applying evidence base in prevention of cyber and internet-enabled crimes	Knowledgeable Empowered
5 Appropriate communication skills including written and oral communication.	Knowledgeable Empowered Engaged

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

Completion of 96 units

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

Students will participate in continuous peer and self-assessment during tutorials. Task 2 will provide feedback for Task 3.

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	Artefact - Creative	Individual	30%	Equivalent to A3 size Approximately 1000 words	Week 4	Online Assignment Submission with plagiarism check
All	2	Case Study	Individual	20%	500 word referenced podcast script outline of selected cybercrime case	Week 7	Online Assignment Submission with plagiarism check
All	3	Case Study	Individual	50%	10 minute podcast episode recording with script and a 500 word reflection	Week 13	Online Assignment Submission with plagiarism check

All - Assessment Task 1: Digital Poster

GOAL:	The purpose of the poster is for you to outline the prevalence and impact of cyber crime or internet enabled crime, and explore the typical characteristics of offenders and victims.													
PRODUCT:	Artefact - Creative													
AUTHORSHIP STATEMENT:														
FORMAT:	Individual digital poster examining the prevalence, impact and characteristics of cyber/internet-enabled crime.													
CRITERIA:	<table border="1"> <thead> <tr> <th>No.</th> <th></th> <th>Learning Outcome assessed</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Description and understanding of prevalence and impact of cybercrime</td> <td>2</td> </tr> <tr> <td>2</td> <td>Description and characteristics of cybercrime type</td> <td>2</td> </tr> <tr> <td>3</td> <td>Appropriate research, design and communication skills.</td> <td>1 5</td> </tr> </tbody> </table>	No.		Learning Outcome assessed	1	Description and understanding of prevalence and impact of cybercrime	2	2	Description and characteristics of cybercrime type	2	3	Appropriate research, design and communication skills.	1 5	
No.		Learning Outcome assessed												
1	Description and understanding of prevalence and impact of cybercrime	2												
2	Description and characteristics of cybercrime type	2												
3	Appropriate research, design and communication skills.	1 5												
GENERIC SKILLS:	Communication, Information literacy													

All - Assessment Task 2: True Crime Podcast - Outline

GOAL:	The purpose of this task is to provide an script outline for a podcast using a real cybercrime case.																
PRODUCT:	Case Study																
AUTHORSHIP STATEMENT:																	
FORMAT:	Individual written assessment of an podcast episode outline. Students are required to complete this task using Cadmus.																
CRITERIA:	<table border="1"> <thead> <tr> <th>No.</th> <th></th> <th>Learning Outcome assessed</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Demonstration of relevant cybercrime knowledge around methods and prevention of cybercrime types</td> <td>2 4</td> </tr> <tr> <td>2</td> <td>Appropriate use of research and open-source evidence</td> <td>1</td> </tr> <tr> <td>3</td> <td>Application of relevant criminological theory to cybercrime case</td> <td>3</td> </tr> <tr> <td>4</td> <td>Demonstrates academic integrity, appropriate communication skills, and meets word count</td> <td>5</td> </tr> </tbody> </table>	No.		Learning Outcome assessed	1	Demonstration of relevant cybercrime knowledge around methods and prevention of cybercrime types	2 4	2	Appropriate use of research and open-source evidence	1	3	Application of relevant criminological theory to cybercrime case	3	4	Demonstrates academic integrity, appropriate communication skills, and meets word count	5	
No.		Learning Outcome assessed															
1	Demonstration of relevant cybercrime knowledge around methods and prevention of cybercrime types	2 4															
2	Appropriate use of research and open-source evidence	1															
3	Application of relevant criminological theory to cybercrime case	3															
4	Demonstrates academic integrity, appropriate communication skills, and meets word count	5															
GENERIC SKILLS:	Communication, Problem solving, Information literacy																

All - Assessment Task 3: True Crime Podcast - Episode with Reflection

GOAL:	The purpose of this task is to provide a podcast episode of a true cybercrime case study, summarising details of the case, applying a theory to describe how/why the crime occurred, and outlining how similar crimes can be prevented.																			
PRODUCT:	Case Study																			
AUTHORSHIP STATEMENT:																				
FORMAT:	Individual assessment consisting of 10 minute audio recording of podcast episode and written 500 word reflection. Students are required to complete this task using Cadmus.																			
CRITERIA:	<table border="1"><thead><tr><th>No.</th><th></th><th>Learning Outcome assessed</th></tr></thead><tbody><tr><td>1</td><td>Explanation of the methods used to commit cyber crime</td><td>2</td></tr><tr><td>2</td><td>Application of theory to explain cyber crime opportunity</td><td>3</td></tr><tr><td>3</td><td>Appropriate use of research and open source evidence</td><td>1</td></tr><tr><td>4</td><td>Identification and discussion of prevention methods</td><td>4</td></tr><tr><td>5</td><td>Demonstrates academic integrity, appropriate communication skills, and meets time and word count</td><td>5</td></tr></tbody></table>	No.		Learning Outcome assessed	1	Explanation of the methods used to commit cyber crime	2	2	Application of theory to explain cyber crime opportunity	3	3	Appropriate use of research and open source evidence	1	4	Identification and discussion of prevention methods	4	5	Demonstrates academic integrity, appropriate communication skills, and meets time and word count	5	
No.		Learning Outcome assessed																		
1	Explanation of the methods used to commit cyber crime	2																		
2	Application of theory to explain cyber crime opportunity	3																		
3	Appropriate use of research and open source evidence	1																		
4	Identification and discussion of prevention methods	4																		
5	Demonstrates academic integrity, appropriate communication skills, and meets time and word count	5																		
GENERIC SKILLS:	Communication, Problem solving, Organisation, Applying technologies, Information literacy																			

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

There are no required/recommended resources for this course.

8.2. Specific requirements

Not applicable

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:

- (a) The final mark is in the percentage range 47% to 49.4%; and
- (b) The course is graded using the Standard Grading scale

10.3. Assessment: Submission penalties

Late submissions may be penalised up to and including the following maximum percentage of the assessment task's identified value, with weekdays and weekends included in the calculation of days late:

- (a) One day: deduct 5%;
- (b) Two days: deduct 10%;
- (c) Three days: deduct 20%;
- (d) Four days: deduct 40%;
- (e) Five days: deduct 60%;
- (f) Six days: deduct 80%;
- (g) Seven days: A result of zero is awarded for the assessment task.

The following penalties will apply for a late submission for an online examination:

Less than 15 minutes: No penalty

From 15 minutes to 30 minutes: 20% penalty

More than 30 minutes: 100% penalty

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

For course-specific questions, contact your teaching staff or Course Coordinator.

For other enquiries or to access support, please contact Student Central:

- [UniSC Student Central](#)
- [UniSC Adelaide Student Central](#)