COURSE OUTLINE

CRM310 Introduction to Cyber Crime

School: School of Law and Society

2022 | Semester 1

UniSC Sunshine Coast	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.

Please go to usc.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 cyber environment in which the cyber security professional, cybercriminal lawyer, and cybercriminal operates. This course develops your knowledge of cybercrime, technical writing skills, analytical skills and the digital collaboration skills needed to prepare you for the following technical cyber security courses. You will learn about the cybersecurity field, what motivates cybercriminals, how individuals, groups and state-sponsored organisations operate, and how cyber criminals target individuals and businesses, unlawfully seizing data and identities. You will also be introduced to darknet markets where stolen data, identities and intellectual property is traded and how international law enforcement agencies operate to locate and prosecute cyber criminals.

1.2. How will this course be delivered?

ACTIVITY	HOURS	BEGINNING WEEK	FREQUENCY
BLENDED LEARNING			
Learning materials – Online learning materials for 13 weeks (or equivalent).	1hr	Week 1	13 times
Seminar – On campus seminar - 2 hours in weeks 1 and 8	2hrs	Week 1	2 times
Tutorial/Workshop 1 – On campus tutorial - 2 hours in weeks 2-7 and weeks 9-13	2hrs	Week 2	11 times
ONLINE			
Learning materials – Online learning materials for 13 weeks (or equivalent).	1hr	Week 1	13 times
Seminar – Recording of on campus seminar - 2 hours in weeks 1 and 8. Recording will be made available after on-campus seminar.	2hrs	Week 1	2 times
Tutorial/Workshop 1 – Tutorial via Zoom - 2 hours in weeks 2-7 and weeks 9-13	2hrs	Week 2	11 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. 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,
- Hacking,
- The dark net,
- Enforcement and investigation,
- Cybersecurity and prevention.

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 On successful completion of this course, you should be able to...	GRADUATE QUALITIES Completing these tasks successfully will contribute to you becoming...
1	Appropriate use of research evidence and communication skills.	Empowered
2	Identify and explain the range of methodologies cybercriminals use to undertake and complete cyber and internet-enabled crimes	Empowered
3	Identify and discuss the physical, social and societal costs to individuals and the community from cybercrime events.	Sustainability-focussed
4	Understand and apply criminological theories to cybercrime	Knowledgeable Creative and critical thinker
5	Analysing and applying evidence base in prevention of cyber and internet-enabled crimes	Knowledgeable Empowered

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

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 during tutorials

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 - Technical and Scientific, and Written Piece	Individual	30%	Maximum 1,000 words	Week 4	Online Assignment Submission with plagiarism check
All	2	Case Study	Individual	40%	2,000 words	Week 9	Online Assignment Submission with plagiarism check
All	3	Oral	Individual	30%	5-7 minute presentation	Refer to Format	Online Assignment Submission with plagiarism check and in class

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 - Technical and Scientific, and Written Piece
FORMAT:	Digital poster examining the prevalence, impact and characteristics of cyber/internet-enabled crime.
CRITERIA:	

No.		Learning Outcome assessed
1	Description and understanding of prevalence and impact of cybercrime	3
2	Description and characteristics of cybercrime type	2
3	Appropriate research, design and communication skills.	1

All - Assessment Task 2: Hacker Case Study Written Report

GOAL:	The purpose of this task is to provide a written profile of a case study: profiling the hacker/s, summarising the details of the case, explaining the techniques involved, and applying a theory to describe how and why the crime occurred.
PRODUCT:	Case Study
FORMAT:	This case study will require you to use information covered in the course and open sources (e.g., news articles) to examine the aspects of a specific case.

CRITERIA:

No.		Learning Outcome assessed
1	Explanation of the methods used to commit cyber crime	2
2	Application of theory to explain cyber crime opportunity	4
3	Appropriate use of research and open source evidence	1

All - Assessment Task 3: Cybercrime Prevention

GOAL:	The goal of the task is to examine a specific type of cyber or internet-enabled crime and discuss how it is undertaken and how it can be prevented.
PRODUCT:	Oral
FORMAT:	5-7 minute presentation in tutorial outlining prevention of a cyber or internet-enabled crime. Slides to be submitted in week 11 with presentations to occur in class during week 12 or 13.

CRITERIA:

No.		Learning Outcome assessed
1	Identification of the method/s offenders use to undertake specific type of cybercrime	2
2	Identification and discussion of prevention methods	5
3	Professional communication and quality of PowerPoint presentation	1

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

Please note that you need to have regular access to the resource(s) listed below. Resources may be required or recommended.

REQUIRED?	AUTHOR	YEAR	TITLE	EDITION	PUBLISHER
Required	Jonathan Clough	2015	Principles of Cybercrime	2nd ed	Cambridge University Press

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

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. SafeUniSC

UniSC is committed to a culture of respect and providing a safe and supportive environment for all members of our community. For immediate assistance on campus contact SafeUniSC by phone: 07 5430 1168 or using the SafeZone app. For general enquires contact the SafeUniSC team by phone 07 5456 3864 or email safe@usc.edu.au.

The SafeUniSC Specialist Service is a Student Wellbeing service that provides free and confidential support to students who may have experienced or observed behaviour that could cause fear, offence or trauma. To contact the service call 07 5430 1226 or email studentwellbeing@usc.edu.au.

10.5. Study help

For help with course-specific advice, for example what information to include in your assessment, you should first contact your tutor, then your course coordinator, if needed.

If you require additional assistance, the Learning Advisers are trained professionals who are ready to help you develop a wide range of academic skills. Visit the Learning Advisers web page for more information, or contact Student Central for further assistance: +61 7 5430 2890 or studentcentral@usc.edu.au.

10.6. Wellbeing Services

Student Wellbeing provide free and confidential counselling on a wide range of personal, academic, social and psychological matters, to foster positive mental health and wellbeing for your academic success.

To book a confidential appointment go to Student Hub, email studentwellbeing@usc.edu.au or call 07 5430 1226.

10.7. AccessAbility Services

Ability Advisers ensure equal access to all aspects of university life. If your studies are affected by a disability, learning disorder mental health issue, injury or illness, or you are a primary carer for someone with a disability or who is considered frail and aged, AccessAbility Services can provide access to appropriate reasonable adjustments and practical advice about the support and facilities available to you throughout the University.

To book a confidential appointment go to Student Hub, email AccessAbility@usc.edu.au or call 07 5430 2890.

10.8. 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

10.9. 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.

10.10. 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