Module Descriptor

Title	Cybercrime and Online Risks		
Session	26/27	**Status**	active
Code	CRIM09026	**SCQF Level**	9
Credit Points	20	**ECTS (European Credit Transfer Scheme)**	10
School	Education and Social Sciences		
Module Co-ordinator	K Cooper		

Summary of Module

This module provides a critical exploration of the sociological, legal, and ethical dimensions of digital criminality and online risk. Students will evaluate the impact of evolving technologies on individuals, organizations, and global infrastructure.
The curriculum focuses on the conceptual 'grey areas' of cyberspace—where technology, human behaviour, and law intersect. Students will develop practical skills in digital risk assessment and the use of open-source information (OSINT) to analyse contemporary threats. This module is designed for students from a non-technical background, emphasising the professional communication and critical thinking skills required to navigate the digital age.

Indicative themes include (subject to change):

- Theoretical frameworks for understanding digital deviance and criminality.
- Analysis of risks to personal privacy, data ethics, and digital identity.
- The role of Open Source Intelligence (OSINT) and publicly available information in cyber investigation.
- Strategies for risk mitigation and professional communication of digital threats.

Module Delivery Method	On-Campus[1] x	Hybrid[2] ☐	Online[3] ☐	Work -Based Learning[4] ☐
Campuses for Module Delivery	☐ Ayr ☐ Dumfries	☐ Lanarkshire ☐ London ☒ Paisley	☐ Online / Distance Learning ☐ Other (specify)	

Terms for Module Delivery	Term 1		Term 2 ☐	Term 3	☐
Long-thin Delivery over more than one Term	Term 1 – Term 2	☒	Term 2 – Term 3 ☐	Term 3 – Term 1	☐

Learning Outcomes	
L1	Demonstrate a broad understanding of how internet-connected technologies are and can be used to facilitate the commission of crimes and antisocial behaviour.
L2	Critically assess the development of ICT and the risks they have in terms of facilitating crime and exposing individuals to crime.
L3	Identify and engage with publicly available and open-source information and appropriate academic sources regarding past and unfolding cyber and ICT incidents.
L4	Evaluate costs and potential costs of a recent cybercrime attack and ongoing cybercrime and deviant activities and develop mitigation strategies.
L5	Communicate and assess complex information in concise, clear, and professional way for generalist audiences using verbal and written communication strategies.

Employability Skills and Personal Development Planning (PDP) Skills	
SCQF Headings	**During completion of this module, there will be an opportunity to achieve core skills in:**
Knowledge and Understanding (K and U)	Students will demonstrate a knowledge of cybercrime, online deviance, and digital security and privacy that is informed by forefront developments and develop a critical understanding of principles, concepts, and terminology related to cybercrime, digital spaces, and online deviant behaviour.
Practice: Applied Knowledge and Understanding	Students will apply knowledge, skills and understanding in using a range of professional skills and techniques applied to professional-level contexts that include a degree of unpredictability and will practice routine methods of enquiry and research.

[1] Where contact hours are synchronous/ live and take place fully on campus. Campus-based learning is focused on providing an interactive learning experience supported by a range of digitally-enabled asynchronous learning opportunities including learning materials, resources, and opportunities provided via the virtual learning environment. On-campus contact hours will be clearly articulated to students.

[2] The module includes a combination of synchronous/ live on-campus and online learning events. These will be supported by a range of digitally-enabled asynchronous learning opportunities including learning materials, resources, and opportunities provided via the virtual learning environment. On-campus and online contact hours will be clearly articulated to students.

[3] Where all learning is solely delivered by web-based or internet-based technologies and the participants can engage in all learning activities through these means. All required contact hours will be clearly articulated to students.

[4] Learning activities where the main location for the learning experience is in the workplace. All required contact hours, whether online or on campus, will be clearly articulated to students

Generic Cognitive skills	Evaluating a range of sources, students will be able to make both snap and considered judgements regarding routine problems and issues in the context of cybercrime, cybersecurity, and cyberdeviance. Students will also undertake critical analysis of issues and synthesize information from a diverse range of sources
Communication, ICT and Numeracy Skills	Students will use a wide range of routine research and communication skills. They will also develop sector-associated skills in terms of searching for information, writing briefs and presenting complex situations to relevant stakeholders.
Autonomy, Accountability and Working with Others	Students will demonstrate professionalism, via producing their work on a regular basis, editing their own work, and providing constructive criticism of their peers' work.

Prerequisites	**Module Code**	**Module Title**
	Other	
Co-requisites	**Module Code**	**Module Title**

Learning and Teaching	
In line with current learning and teaching principles, a 20-credit module includes 200 learning hours, normally including a minimum of 36 contact hours and maximum of 48 contact hours.	
Learning Activities During completion of this module, the learning activities undertaken to achieve the module learning outcomes are stated below:	**Student Learning Hours** (Note: Learning hours include both contact hours and hours spent on other learning activities)
Lecture / Core Content Delivery	12
Laboratory / Practical Demonstration / Workshop	24
Asynchronous Class Activity	12
Independent Study	152
TOTAL	200

Indicative Resources
The following materials form essential underpinning for the module content and ultimately for the learning outcomes: *Baker, R. (2023). Deep Dive: Exploring the Real-World Value of Open Source Intelligence. John

Wiley & Sons.

*Bazzell, M. (2022) Extreme Privacy: What It Takes to Disappear. 4th edn.: Independently Published.

*Lewis, S. J. (ed.) (2017) Queer Privacy: Essays From the Margins of Society: Mascherari Press.

*Powell, A. and Henry, N. (2017) Sexual violence in a digital age. London: Palgrave MacMillan.

*Yar, M. and Steinmetz, K. F. (2023) Cybercrime and Society. Fourth Edition edn. Los Angeles: SAGE.

Students will also be required to read blogs and websites such as Wired and Krebs on Security. Specific blogs and websites will be selected based on what is being maintained at the time the class runs.

(N.B. Although reading lists should include current publications, students are advised (particularly for material marked with an asterisk*) to wait until the start of session for confirmation of the most up-to-date material)

Attendance and Engagement Requirements

In line with the Student Attendance and Engagement Procedure, Students are academically engaged if they are regularly attending and participating in timetabled on-campus and online teaching sessions, asynchronous online learning activities, course-related learning resources, and complete assessments and submit these on time.

For the purposes of this module, academic engagement equates to the following:

The university is committed to providing a supportive learning environment that activelyfacilitates student success. In this module, there is a high degree of student-led flexibility. You are academically engaged if you are regularly engaged with scheduled live sessions on-campus, learning activities in your own time, course-related learning resources, and withtimely completion and submission of assessments. Whilst we understand that there may be times when conflicting priorities make participationchallenging, for you to gain the most from this module it is recommended that you participatein all scheduled live classes and complete your self-directed learning activities in a timely manner.

It may be difficult to pass the assessment associated with this module if you are not regularlyengaging with the module work and live classes. We may reach out to check how things are going and offer support if we observe that you have not been attending sessions orcompleting online activities.

Equality and Diversity

The University's Equality, Diversity and Human Rights Procedure can be accessed at the following link: UWS Equality, Diversity and Human Rights Code.

In line with current legislation (Equality Act, 2010) and the UWS Equality, Diversity, and Human Rights Code, our modules are accessible and inclusive, with reasonable adjustment for different needs where appropriate. Module materials comply with University guidance on inclusive learning and teaching, and specialist assistive equipment, support provision and adjustment to assessment practice will be made in accordance with UWS policy and regulations.

(N.B. Every effort will be made by the University to accommodate any equality and diversity issues brought to the attention of the School)

Supplemental Information

Divisional Programme Board	**Social Sciences**Error! Bookmark not defined.
Overall Assessment Results	☒ **Graded**
Module Eligible for Compensation	**Yes** **If this module is eligible for compensation, there may be cases where compensation is not permitted due to programme accreditation requirements. Please check the associated programme specification for details.**
School Assessment Board	Criminology
Moderator	J Miller
External Examiner	Morena Tartari
Accreditation Details	
Module Appears in CPD catalogue	**No**
Changes / Version Number	1

Assessment (also refer to Assessment Outcomes Grids below)
Assessment 1 Portfolio
Assessment 2 Presentation
Assessment 3
(N.B. (i) Assessment Outcomes Grids for the module (one for each component) can be found below which clearly demonstrate how the learning outcomes of the module will be assessed. (ii) An indicative schedule listing approximate times within the academic calendar when assessment is likely to feature will be provided within the Student Module Handbook.)

Component 1							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
Portfolio	**x**Error! Bookmark not defined.	**x**				60%	

Component 2							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**

Presentation			**x**	**x**		40%	

Component 3							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
	☐	☐	☐	☐	☐		
Combined total for all components						100%	hours

Change Control

What	**When**	**Who**