MODULE DESCRIPTOR

TITLE	ELECTRONIC CRIME			
SI MODULE CODE	25-7A18-00S/N			
CREDITS	15			
LEVEL	7			
JACS CODE	G500 - Information Systems			
SUBJECT GROUP	Business Operations and Financial Info Systems			
DEPARTMENT	Finance, Accounting and Business Systems			
MODULE LEADER	Lucian Tipi			
NOTIONAL STUDY HOURS BY TYPE	Tutor-led	Tutor-directed	Self-directed	Total Hours
	30	60	90	180

MODULE AIM(S)

This module will enable students to:

To develop an understanding of the major software applications most commonly in use for accounting, finance, business management and international commercial networks.

To facilitate the identification and understanding of the major types of commonly-encountered electronic crime.

To develop an appreciation of risk assessment processes for electronic systems.

To enable participants to identify computer security and control systems appropriate to given situations.

To enable participants to gain an appreciation of major software applications for computer audit and interrogation.

To develop an understanding of the collection of electronic information for evidence production purposes.

MODULE LEARNING OUTCOMES

By engaging successfully with this module a student will be able to

On successful completion of the module students will be able to:

- Demonstrate an awareness of the major business-related software applications,
- Identify the major types of commonly-encountered electronic crime,
- Demonstrate an appreciation of risk assessment processes for electronic systems,
- Identify computer security and control systems appropriate to given situations,
- Demonstrate an appreciation of major software applications for computer audit and interrogation,
- Demonstrate an understanding of the collection of electronic information for evidence production purposes.

INDICATIVE CONTENT

These are examples of the content of the module

The module will cover a broad range of topics in the very fast moving area that is the Electronic Crime area. An indicative list of topics can be found in the following:

- Vulnerabilities of and threats to Information Systems within organisations, the commercial use of the Internet, Information Systems infrastructure;

- History and developments of electronic crime, e.g. malware, denial of service and distributed denial of service, hacking, spyware, etc.
- Frameworks for classifying electronic crime;
- Legislation and associated cases;
- Government and commercial initiatives for Information Systems governance and security;
- Digital forensics and electronic evidence;
- Software applications for digital forensics;
- Social impact and the future of electronic crime.

This is not an exhaustive list; other topics/issues will be discussed during the module with relevant examples presented as they will be identified during the running of the module. Relevant current case studies will be utilized as appropriate.

LEARNING AND TEACHING METHODS

Students will be supported in their learning, to achieve the above outcomes, in the following ways

The module will be delivered by a series of sessions which will have a lecture element followed by a seminar element – so called “lectorial” sessions. Also the sessions will contain a significant element of student led discussions. The lecture element will deliver the core theoretical material of the module and this will be then augmented with case studies, examples and activities in the seminar element.

Some of the module sessions will be student led and will be based on discussions around topical areas of electronic crime; the sessions will explore topical issues related to the core material of the module as well as the assessment package of the module.

A student led presentation session, based on research into key topics, will be a feature of the module. Oral formative feedback will be provided at the end of the presentations, to prepare students for their coursework.

The module Blackboard site is central to the delivery of the module as it will contain a broad range of electronic materials, including the lecture slides and the seminar exercises. There is an intention to bring in guest speakers as appropriate. A number of drop in style sessions will be run in order to provide support with the coursework.

ASSESSMENT STRATEGY AND METHODS

The assessment tasks and will be presented in this section.

Assessment Task		Contribution to the module mark
Task 1	An Individual Written Assessment (4500 words equivalent)	100%

Task 1 – the Individual Written Assessment will be an evaluation piece on a topic that will be decided following the discussions between the module leader and the students. A choice of several topics will be given to students and then based on the in sessions discussions a topic will be chosen. All students will then need to work on the chosen topic.

Support with the assessment tasks will be provided throughout the module and therefore it is important that students make sure to engage with the module throughout.

Task No.	Task Description	Task Type	Task Weighting %	Word Count / Duration	In-module retrieval available
1	Individual Written Coursework	Coursework	100	4500 words	No

ASSESSMENT CRITERIA

The general module assessment grid for is presented in the following table:

Learning Outcome		**40-49%**	**50-59%**	**60-69%**	**>70%**
Outcomes 1 and 2	Material imported from other sources	Tendency to be descriptive	Sound analysis	Critical and reasoned analysis	Perceptive and insightful analysis
	No issues identified	Some issues identified	Identification of some key issues	Identification of key issues	Identification of key and potential issues
	No knowledge of the topic	Limited knowledge of topic	Clear knowledge of topic	Good knowledge of topic	Excellent understanding of topic
	No literature review	Weak literature review	Sound literature review	Critical consideration of literature	Perceptive critique of literature
	No attempt to conclude	Some attempt to conclude	Competent attempt to conclude	Critical and reasoned conclusion	Perceptive and insightful conclusions
Outcomes 3,4,5 and 6	No application to the situation	Limited application to situation	Competent attempt to relate to situation	Reasoned application to situation	Insightful application to situation

FEEDBACK

Students will receive feedback on their performance in the following ways

Both formative and summative feedback will be provided to students as follows:

Formative feedback:

- Formative feedback will be provided by the teaching team on an on-going basis throughout the duration of the module; the module Blackboard site will be used as a vehicle for this also;
- At least one session per semester during the delivery of the module will be dedicated to providing formative feedback to students in its entirety. These will take the form of drop in style sessions.
- Students will be encouraged throughout the delivery of the module to seek clarifications on the topics being presented and to bring their own discussion points to the table – the ensuing discussions with the tutor and the rest of the class will also for an important part of the formative feedback given to students.

Summative feedback:

- Written feedback following the submission of Assessment Task 1 will be made available by the module team as per the Assessment and Feedback regulations.

LEARNING RESOURCES (INCLUDING READING LISTS)

The module leader liaises closely with the university learning centre to ensure a wide variety of the latest books and articles are available to aid your studies. Students will also be able to utilise the online journals database via the learning centre website. The module guide will outline key readings along with utilising the Talis reading list system.

The module will be heavily reliant on the module Blackboard site as the means for disseminating all of the materials necessary in an electronic format. The materials posted on the module Blackboard site will include the lecture slides, the seminar activities, various case studies utilized throughout the module and also links to a variety of web resources, as needed.

The module Blackboard site will also be used extensively for communicating with students.

Printed materials will be provided to students in the form of module guide, hand-outs for the seminar component of the sessions and case studies when appropriate.

An extensive reading list will be provided to students, as listed below. Due to the very fast moving nature of the issues approached in the module, this reading list will be frequently updated, from one delivery of the module to the other. Although an extensive reading list is provided, students are not expected to read all of the materials provided in this list, but rather to select a range of titles that are appropriate.

Students will need to make extensive use of web resources, particularly when it comes to finding relevant case studies needed to support their discussion.

Reading list (short version):

Laudon and Laudon; Management Information Systems, 12th edition, 2011

Dhillon G.; Principles of Information Systems Security: Texts and Cases, 2006

Kenneth C. Laudon and Carol Guercio Traver; E-Commerce 2010: International Version: Business, Technology, Society, 6th edition, 2009

Austin R. and Darby C. A. R.; The Myth of secure computing; Harvard Business Review, 2009

Portnoy M. and Goodman S.; Global Initiatives to Secure Cyberspace: An Emerging Landscape (Advances in Information Security), 2010

Khalfan S.; Managing internal and external risk in the information age, 2009

Coderre D.; Computer Aided Fraud Prevention and Detection: A Step by Step Guide, 2009

Web Resources

http://www.zdnet.com

http://www.getsafeonline.org

http://www.itgovernance.co.uk

http://www.bis.gov.uk/policies/business-sectors/information-security

http://www.bbc.co.uk/news