Aims
This module complements other modules by examining the subject from the criminal angle and presenting a study of cybercrime and the cyber criminal. It covers the history, causes, and development of cybercrime through studies of surveys, types of crime, legal measures, and system and human vulnerabilities. It will also examine the effects of cybercrime through the experiences of victims and law enforcement and look at the motives and attitudes of hackers and other cyber criminals.

Pre-requisites
None

Essential Reading
- Information Warfare and Security (D Denning) Addison Wesley 1998
- Cybercrime: The transformation of crime in the Information Age (D Wall) Polity Press 2007
- Information Technology Law (I Lloyd) Oxford University Press 2011

Included as study material once registered on the course.

Assessment
This module is assessed by a two hour unseen written examination.

Learning Outcomes
On completion of the module students should be able to:

- follow trends in cybercrime
- relate computer security methodologies to criminal methods
- detect criminal activity in a computerised environment
- apply the criminal and civil law to computer criminality
- understand how viruses, logic bombs and hacking are used by criminals
- appreciate the views of the public, business, governments, and the media to occurrences of cybercrime.
- understand the need to gather and preserve digital evidence correctly so that legal actions can be brought

Syllabus

Unit 1 - Setting the Scene
This unit starts with a short overview. It then discusses some basic definitions and looks at the problem of evaluating sources (which is a skill needed for the entire module).

Unit 2 - Analysing Cybercrime
This unit looks at the perception and impact of information crime on different aspects of society, as well as different types of cybercrime.
Unit 3 - Principles of Law and Computer Misuse
This unit provides a short introduction to the relevant aspects of law necessary to interpret information crime. It then goes on to examine the most important piece of legislation in the U.K. dealing specifically with cybercrime, the Computer Misuse Act 1990. Other acts discussed include the Fraud Act 2006, Communications Act 2003 and laws concerning abusive images of children.

Unit 4 - Computer Hacking
This unit examines the growth of the culture of computer hacking and the methodologies and techniques used to gain illegal access to systems.

Unit 5 - Traditional Cybercrime
This unit looks at a number of traditional forms of crime and examines how they manifest themselves as cybercrimes.

Unit 6 - Psychological Cybercrime
This unit examines psychological cybercrimes such as fabrication, hoaxes, distortions, defamation and social engineering.

Unit 7 - Telecommunications Crime
The information society relies on telecommunications as an underlying technology, provides an overview of telecommunications crimes and discusses related legislation.

Unit 8 - Viruses and Worms
This unit focuses on understanding the effects of malware such as viruses and worms, how they spread and the damage they can do.

Unit 9 - Denial of Service Attacks
A denial of service attack on a computer system is an attack on its availability and can be undertaken for various criminal reasons. This unit examines denial of service attacks in the context of cybercrime.

Unit 10 - Digital Evidence
This unit aims to provide an understanding of what digital evidence is, and how it can be gathered in a manner that is suitable for use in an investigation. An investigation may be civil, criminal or disciplinary, that is, it may be brought by the Crown against an individual, by a private party, or by an employer. The strictest standard for evidence is that it is suitable for use in a criminal court.