



University of London International Academy  
MSc/PG Dip in Information Security  
Lead College – Royal Holloway

## Cybercrime IYM010 (Option)

### Aims

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

### Pre-requisites

None

### Essential Reading

- Cybercrime: The transformation of crime in the Information Age (D.S Wall) Polity Press 2007
- Computer Crimes & Digital Investigations (I Walden) Oxford University Press 2007

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 computer crime
- 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 business, governments, and the media to instances of computer crime.
- 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 information crime.

**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 information crime, the Computer Misuse Act 1990 and changes made to it in the Police and Justice Act 2006 and the Serious Crime Act 2007 (SCA).

**Unit 4 - Computer Hacking**

This unit examines the growth of the culture of computer hacking and some of its methodologies

**Unit 5 - Traditional Cybercrime**

This unit looks at a number of traditional forms of crime and examines how they manifest themselves as information crimes.

**Unit 6 - Psychological Information Crime**

This unit examines psychological information crimes such as fabrication, hoaxes, distortions, defamation and social engineering.

**Unit 7 - Telecommunications Crime**

The information society relies on

telecommunications as an underlying technology. This unit provides an overview of telecommunications crimes and discusses related legislation.

**Unit 8 - Viruses and Worms**

This unit focuses on understanding the effects of viruses and worms, which represent a high profile and familiar manifestation of what can sometimes be an information crime.

**Unit 9 - Denial of Service Attacks**

Another high profile type of attack on a computer system is an attack on its availability. This unit examines denial of service attacks in the context of information crime.

**Unit 10 – Digital Evidence**

This unit aims to provide you with 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.