INFORMATION SECURITY GROUP

Course Specification 2013-14

Code:	IY5605	**Course Value:**	0.5	**Status:**	Option
Title:	**Cyber Crime**			**Availability:**	Spring Term
Prerequisites:	Core courses			**Recommended:**	None
Co-ordinator:	John Austen				
Course Staff	John Austen				
Aims:	This course will: • complement other information security courses by examining the subject from the criminal angle • investigate the history and causes of computer crime • examine the effects of computer crime through the experiences of victims and law enforcement • consider the technologies that stand behind certain computer crimes, namely malware (viruses, worms, Trojan Horses, etc.), email spamming and denial of service (DoS) attacks.				
Learning Outcomes:	On successful completion of the course students will be able to: ▪ identify and evaluate 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 ▪ explain how malware and other technical hacking techniques are used by criminals ▪ understand the mechanisms hackers use to social engineer their victims ▪ assess the mechanisms used to launch DoS and distributed DoS attacks and propose suitable countermeasures ▪ compare and evaluate the views and responses of business, governments, and the media to instances of computer crime.				
Course Content:	▪ Introduction: Types of computer crime, history, surveys, statistics and global connections ▪ Legal Measures: Computer Misuse, Criminal Damage, Software Piracy, Forgery, Investigative Powers ▪ Case Studies: Investigations into hacking, cases and PC misuse ▪ Social Engineering ▪ Spam, Phishing and Pharming ▪ Malware: The types, effects, and investigations ▪ DoS and Distributed DoS: The causes, mechanisms, case studies, and countermeasures ▪ Network Crimes: Hacking methodologies via the Internet and attacks to other networks ▪ Investigations, incident handling and forensic examination ▪ The Future: The expansion of the Internet, pornography and other unsuitable material. ▪ Identity Theft and Fraud				
Teaching & Learning Methods	Eleven 3-hour presentations with handouts and additional press material, web references, video clips, and live demonstrations.				
Key Bibliography:	Blackstone's Statutes on IT and E-Commerce, Oxford University Press. C. Stoll, The Cuckoo's Egg, Pan Book. Various web-sites including Sans Newsbytes and Sophos Naked Security.				
Formative Assessment and Feedback:	Multiple revision tutorials are given during which computer crime scenarios are discussed from an examination perspective. Also, tutorial sessions are used to provide feedback on student answers to exercise sheets.				
Summative Assessment:	**Exam** 100(%) This course is assessed solely by written examination consisting of a two-hour-exam. *(3 out 5 questions)* **Coursework** 0(%) Coursework does not contribute to the final assessment for this course. **Deadlines:** The written examination will be held in the Summer term				