

FOR 360 – Cybercrime (Fall 2008, Dublin)

Contact Information

Name	Owen O'Connor
Email	OConnor@Champlain.edu
Telephone	+353 1 524 2407 (office)
For queries or issues	Email generally preferred, will also aim to be available 30 minutes before the beginning of each class, can arrange to meet at other times if needed.

Course Information

Course Title	Cybercrime
Course Number	FOR360
Course Description	This course will focus on economic and other crimes perpetrated over the Internet or other telecommunications networks. This course will discuss crimes ranging from auction fraud and social engineering to e-mail scams and phishing. Network forensics and investigative techniques will also be presented.
Topics	<ol style="list-style-type: none">1. Cybercrime landscape & history2. Growth & impact of cybercrime3. Cybercrime legislation & offences4. Law enforcement agencies dealing with cybercrime5. Crime in online venues6. Identity theft, credential theft & account hijacking7. Online fraud and theft of funds8. Data theft & security breach notification9. Public policy and cybercrime10. Child exploitation online11. Cyberstalking & online harassment12. Hacking & intrusion13. Cybercrime & emerging technologies

Student Learning Outcomes

Through reading, discussions, exercises, case studies and a final research project, will:

1. Understand different types of cybercrime and how such activities are perpetrated.
2. Determine what actual crime has been committed and in what jurisdiction for a given incident.
3. Compare and contrast the various types of cybercrime.
4. Discuss important aspects of computers and the Internet relative to crime online.
5. Identify the key agencies involved in cybercrime investigations worldwide.
6. Analyze case studies involving collaborative investigation.
7. Describe the critical aspects of a variety of types of crime that exist in the virtual world.
8. Discuss some countermeasures to ensure online safety.

Textbooks

Required Text

Digital Crime and Digital Terrorism
Taylor, Robert
ISBN 0-13-114137-6
Prentice Hall (March 11, 2005)

Supplemental reading material will be prescribed throughout the course.

Participation, Homework & Grading

Participation in this course is important, not only because of the breadth of information to be presented but also because there will be material discussed in class which may not be reflected in notes or textbooks. Full attendance is therefore expected, as is active participation in class discussions. If you are unable to attend a particular scheduled class please make this known ahead of time as it may be possible to re-schedule classes. An evaluation of contributions to classroom and online discussion will be included in the final grade for this module.

Homework and other assignments will be given throughout this course, as follows:

Exercises

In support of discussions on the cybercrime landscape and the growth and impact of cybercrime, students will analyse a number of examples of public research data on cybercrime, for example the PWC / DTI "Information Security Breaches Survey 2008" from the UK and the Verizon Business "2008 Data Breach Investigation Report". Students will examine individual data elements within the reports as well as summarising and contrasting their findings. In addition students while discussing "Cyberstalking & online harassment" students will be asked to propose approaches to investigate specific scenarios, including methods of obtaining digital evidence, business records etc which would support a criminal prosecution.

Case Study

To follow-on from the discussion of crime in online venues and investigative agencies dealing with cybercrime, students will be asked to identify examples of crimes occurring in specific online environments, identify the various agencies which might have responsibility for responding to such crimes, and develop approaches to engaging law enforcement on behalf of various stakeholders.

Research Paper & Presentation

Building on their study of cybercrime legislation and offences, examples of cybercrime, breach notification principles and public policy issues around cybercrime, students will prepare a paper proposing 3 potential governmental responses to cybercrime which they will present to the class for discussion. Examples might include enacting new legislation, introducing or strengthening mandatory sentencing guidelines, increasing resources to various elements of the criminal justice system, investing in public awareness campaigns, engaging with industry or academia, etc.

Grade Calculation

Final grades will be determined as follows:

Graded Element	Weight
Contribution to class & online discussion	10%
Exercises: cybercrime research data analysis and cyberstalking scenarios	20%
Case study: online crime	20%
Research paper & presentation	25%
Final exam	25%

Students with Disabilities

Students requiring accommodations for any form of disability should contact the Director of the Dublin campus as soon as possible.

Academic Honesty

In the preparation and presentation of any assigned work-including examinations, tests, quizzes, term papers, reports, themes and other written or oral exercises-every student shall conform to a strict standard of academic honesty. Any attempt to deceive a faculty member or to help another student to do so will be considered a violation of this standard. In all assignments, students must acknowledge the words and/or ideas of others taken from print or electronic media, whether a direct quotation or a paraphrase; any omission of this is dishonest. Cheating on examinations or tests consists of knowingly giving, receiving or using-or attempting to give, receive or use- unauthorized assistance during an examination or test. A faculty member may record a grade of "zero" for any assignment on which a student has plagiarized or cheated. For repeat offenses within a single course, the faculty member may record a grade of "F" for the course. Violations of this policy in multiple courses may result in dismissal from the College. A student may appeal these decisions according to the Academic Grievance Procedure.

Course Calendar

Week Commencing	Topic	Required Reading	Assignment
September 1 st	Cybercrime landscape & history	Chapters 1 & 2	Summarise findings from PWC / DTI & Verizon reports
September 8 th	Growth & impact of cybercrime		Compare PWC & Verizon samples, findings on cost of breaches, findings on insider versus outside incidents
September 15 th	Cybercrime legislation & offences	Chapter 9	
September 22 nd	Crime in online venues		Select an online venue discussed in class & identify examples of crimes occurring in that environment
September 29 th	Law enforcement agencies dealing with cybercrime	Chapter 10	Based on scenarios provided, identify agencies responsible for crimes involved (in each country) and develop an approach for engaging law enforcement
October 6 th	Identity theft, credential theft & account hijacking		
October 13 th	Online fraud and theft of funds	Chapter 5	
October 20 th	Data theft & security breach notification	Chapter 13	
October 27 th	Public policy and cybercrime	Chapter 3	Prepare shortlist of potential proposals to be outlined in research paper / presentation (for approval)
November 3 rd	Child exploitation online		
November 10 th	Cyberstalking & online harassment	Chapter 7	Based on scenarios provided, propose an approach to investigating cyberstalking, including acquisition of evidence required to support a criminal prosecution.
November 17 th	Hacking & intrusion	Chapters 6 & 8	
November 24 th	N/A – Thanksgiving break	N/A	N/A
December 1 st	Cybercrime & emerging technologies	Chapter 14	Research paper due
December 8 th	Presentations		Presentation to be delivered
December 15 th	N/A – exams	N/A	N/A