SEC231 E-crime

Level: 2

Credit Units: 5 Credit Units

Language: ENGLISH

Presentation Pattern: EVERY JAN

Synopsis:

University graduates in Security Studies and those in the private and public sector Security Industry would benefit from being conversant with the issues, problems, and technologies involved in cybercrime and cyber investigations conducted online. SEC231 E-Crime will equip graduates with the requisite knowledge and skills relating to the kinds of criminal activities, methods and instruments used in solving crime as well as formal investigation techniques used in Singapore. A broad range of topics, covering Security Studies concepts of cyber-criminology, criminal behavior,assessment of risk, crime cases, as well as criminal investigation techniques in Southeast Asia. Such knowledge and skills would be highly useful for those already or considering work in the Security Industry in terms of the Singapore Government's Security Industry Transformation Map (SITM).

Topics:

- Review the scholarship on online crime and criminal behaviour
- Assess how criminals make use of the Internet to commit crime
- Malware and Cybercriminal Investigation in Singapore and Southeast Asia
- E-crime, e-risk hacking and hackers' egos
- Criminology Models in Online and Offline Crime
- Contrast the kinds of social media platforms used by cybercriminals in South Asia, Southeast Asia, Korea, Japan or China
- e-Commerce, e-Crime and e-Solutions
- Stalking, Bullying and Grooming
- Real World Crime and Virtual World Crime
- Online Criminal Target Selection and Vulnerable Communities
- Investigating Online Crime and Cyber Risk Mitigation Strategies
- Symmetrical Encryption and Asymmetrical Encryption in Online Crime

Textbooks:

Hate Crimes in Cyberspace Danielle Keats Citron Harvard University Press
ISBN-13: 9780674744653

SEC231 - Study Guide
ISBN-13: SG-1795

Learning Outcome:

- Cite the scholarship on crime and criminology
- Classify how criminals make use of the Internet to commit crime
- Contrast the use of different kinds of malware used by criminals to penetrate personal information (e.g. credit card data; passport data; online banking data) in Singapore, Southeast Asia and/or across the world); and how these crimes are investigated
- Associate what motivates hackers and how they break through firewalls
- Discuss the main models used in criminology including Online and Offline Crime
- Distinguish the kinds of social media platforms used by cybercriminals in South Asia, Southeast Asia, Korea, Japan or China
- Estimate the limitations of e-Crime
- Explain the differences between stalking, bullying and grooming in Cybercrime
- Generalize real world crime and virtual world crime in terms of human trafficking, drug trafficking or money laundering.
- Review how cybercriminals select their targets and suggest why certain online communities are more vulnerable than others
- Research cybercrime legislation in Singapore including the Computer Misuse and Cybersecurity Act
- Infer how symmetric encryption systems become vulnerable to cyber criminals
- Rank the levels of online crime that are associated with illegal Internet use
- Distinguish between the Tor Project and the Deep Web
- Identify the physical trigger points of vulnerability across networks

Assessment Strategies - Regular Semester (Evening Class):

Components	**Description**	**Weightage Allocation (%)**
Overall Continuous Assessment	PRE-CLASS QUIZ 1	2
	PRE-CLASS QUIZ 2	2
	GROUP BASED ASSIGNMENT 1	20
	PARTICIPATION 1	6
	TUTOR-MARKED ASSIGNMENT 1	20
Overall Examinable Components	Written Exam	50
Total		**100**

*The information listed is subject to review and change.