PSS309 Cybercrime

Level: 3
Credit Units: 5 Credit Units
Language: ENGLISH
Presentation Pattern: EVERY JULY

Synopsis:

PSS309 Cybercrime covers the developments in cybercrime, focusing on the multiple threats caused by such activities. By examining the nature, prevalence, scope and means by which criminals perform these crimes, students will be able to appreciate the challenges in investigating, prosecuting and preventing cybercrime. This course also examines related crimes such as cyberwarfare and cyberterrorism. The continuous advancements in technology will be reviewed, including the advent of dark nets and crypto currencies. Students will be exposed to industry-related challenges and issues. Students will also gain understanding on the impact of cybercrime on victims, businesses, and the state, as well as learn about the roles and responsibilities of the different stakeholders in preventing cybercrime. Their knowledge and skills will be assessed based on their ability to manage and solve industry-related issues.

Topics:

- Introduction to cybercrime
- Laws related to cybercrime
- The evolution of cybercrime
- Theories related to cybercrime
- Understanding threats related to cybercrime
- The interconnected nature of cybercrime
- Detecting cybercrime
- Prosecuting cybercrime
- Dark nets
- Crypto currency
- Computer technology as weapon of mass destruction
- Cyberterrorism

Learning Outcome:

- Examine cybercrime and the regulation of the internet
- Analyse the challenges relating to cybercrime
- Appraise the impact of cybercrime
- Distinguish the forms of cybercriminal activities
- Evaluate the effectiveness of cybercrime policies
- Formulate strategies to detect and prevent cybercrime threats

Assessment Strategies (Daytime Class):

Components	Description	Weightage Allocation (%)
Overall Continuous Assessment	PRE-COURSE QUIZ 1	5

Overall Continuous Assessment	TUTOR-MARKED ASSIGNMENT 1	25
	GROUP BASED ASSIGNMENT 1	15
	DISCUSSION BOARD 1	5
Overall Examinable Components	ECA	50
Total		**100**