**Unit 1:**

1. Define cybercrime and provide your understanding of its nature.
2. Briefly explain the classification of cybercrimes, detailing each category.
3. Identify and describe the various types of cybercriminals.
4. Distinguish between "cybercrime" and "cyber fraud," offering a clear explanation.
5. Illustrate the dissemination of viruses, utilizing diagrams for clarification.
6. Craft a concise commentary on the "Indian Legal Approach to Cybercrime," incorporating both chapter content and additional research.
7. Examine the relevance of cybercrime within the extended enterprise context, elaborating on its implications.
8. Express your comprehension of the global collaboration essential for combatting cybercrime.

**Unit 2:**

1. Elaborate on the classification of cybercrimes, accompanied by relevant examples.
2. Contrast passive and active attacks, citing instances to enhance understanding.
3. Define and explore the concept of social engineering.
4. Investigate cyber stalking and assess its classification under the Indian IT Act.
5. Analyze the role of Botnets in fueling cybercrime, providing insights through explanation.
6. Detail the array of attacks launched using attack vectors.
7. Examine the relationship between cloud computing and cybercrime.

**Unit 3:**

1. Exemplify the various "mobility types" using everyday scenarios you're familiar with.
2. Explore the impact of "perception" on people's vulnerability to mobile computing security threats. Propose measures to counteract this issue.
3. Provide illustrative examples to explain potential attacks on mobile/cell phones.
4. Identify the principal security challenges linked to mobile devices concerning credit card fraud and cybercrimes.
5. Delve into the significance of emerging trends like 5G and IoT in shaping the landscape of mobility.
6. Evaluate the implications of the "Bring Your Own Device" (BYOD) trend on organizational security within the realm of mobile devices.