Cyber Crime and Evidence Management

Course Overview

This course explores how a "networked" world has bred new crimes and new responses, and investigates how information and communication technology (ICT) has become a tool, a target, and a place of criminal activity and national security threats, as well as a mechanism of response. This course addresses such questions as how emerging technologies challenge existing laws and criminal procedures; how nation-states regulate criminal conduct across traditional geographic and political boundaries; what reasonable expectations of privacy are in cyberspace; and how control is shifting from traditional mechanisms of law enforcement to new regulatory regimes, including technology.

Specific topics covered include the information environment as crime scene; hacking and unauthorized access; computer use in traditional crimes like financial fraud, drug trafficking, extortion, securities fraud, and political terrorism; identity theft and online fraud; electronic interception, search and seizure, and surveillance, cyber terror, "hacktivism" censorship and free speech; economic espionage; and information warfare.

Target Audience

- Law Enforcement Personnel
- Security Professionals
- Technology Evangelist
- Ethical Hackers
- Penetration Tester
- Anyone Interested in Banking Industry Security Standards like PCI-DSS Compliance.

Course Key Highlights

- Cyber Extortion & Cyber Cheating
- Cyber Warfare & Cyber Terrorism
- Phishing & Hacking
- Online Frauds
- Malware Attacks
- ATM Machine Fraud And Countermeasures
- Payment Cards and Data Security
- Electronic Card Frauds
- Online Transaction Money Fraud

Course Duration: 40 Hours

Course Content

- **Introduction to Cyber Crime: Concepts and Techniques**
- **Channels of Cyber Crimes**
- **Cyber Crime Methods in Digital World**
    - Evidence Collections of Stalking & Cyber Squatting
    - Cyber Extortion & Cyber Cheating
    - Cyber Warfare & Cyber Terrorism
    - Phishing & Online Hacking Fraud Evidences
- **Computer Insecurity Evidences**
    - Internet Crime & Internet fraud
    - User Failures & Causes
    - Failure Bank
- **Computer Hackers Important in Court Evidence**
- **Computer Fraud Protection & Its Evidence Management**
    - Prevention Controls
    - Controls Detection
    - Controls Mitigation
    - Encryption/ Decryption
- **Incident of Cyber crimes**
    - Cyber Crime Reporting
    - Cyber Crime Investigation
    - Cyber Crime Management
    - Evidence Collection & Chain of Custody
    - Cyber Crime Risk Management
    - Forensics Cyber
- **Online Transactions (Concepts, Emerging Trends and Legal Implications)**
- **Payment Cards & Data Security Issues in Court Evidence etc**
- **Modifying Evidences Information Gathering for Court Point of View**
- **Way to Secure the Evidence in Healthy Manner**
- **Countermeasures of Cyber Evidence in Digital World**