ELECTIVE: IV

BEIT804T1 **CYBER SECURITY**

(Theory Credit: 05)

Teaching Scheme:	**Examination Scheme:**
Lecture: 4 Hours/week	**Theory: T (U): 80 Marks T (I): 20 Marks**
Tutorial: 1 Hour/week	**Duration of University Exam. : 03 Hours**

==========

UNIT I:

Introduction: Cyber Crime; definitions, An origin of the Word, cyber crime - and information security, who are criminals? classification of cyber crimes; email spoofing, spamming, cyber defamation, internet time theft, salami attack or salami technique, data diddling, forgery, web jacking, news group spam or crimes emanating from usenet NewsGroup, Industrial spying or Industrial Espionage, hacking, online fraud, Pronography offenses, software piracy, Computer Sabotage, email bombing, mail bombs, usenet NewsGroup as a source of cyber crimes, computer network intrusion, password sniffing, credit crad fraud, identity theft.

UNIT II:

Introduction, categories of cyber crime, how criminals plan the attack: Reconnaissance, passive and active attacks, scamming/scrutinizing gathered information, attack (Gaining and maintaining the system access, Social engineering, classification of social engineering, cyber stalking, types of stalkers, cases reported on cyber stalking, how stalking works? Real life incidents of cyber stalking, cyber cafe and cyber crimes, fuel for cyber crimes, Botnet, attack vector, cloud computing: why cloud computing? types of services, cyber crime and cloud computing.

UNIT III:

Cyber crime: Mobile and wireless devices: Introduction proliferation of mobile and wireless devices trained in mobility, credit card fraud in mobile and wireless computing era - types and technique of credit card fraud, security challenges posed by mobile devices, registry selling for mobile devices, authentication service security - cryptographic security for mobile devices, LDAP security for handheld mobile computing devices, RAS security for mobile devices, Media player control security, networking API security for mobile computing applications, attacks on mobile phone - mobile phone theft, mobile viruses, mishing, vishing, hacking Bluetooth mobile devices, security implications for organizations, managing diversity and proliferation of hand-held devices, unconventional or stealth storage devices threats through cost and stolen devices. Protecting data on lost devices educating the laptop user, organizational measures of handling mobiles, device related security issues, organizational security policies and measures in mobile computing era.

UNIT IV:

Tools and methods used in Cyber crime: Introduction proxy servers and ananymizers phishing, password cracking - online attacks, offline attacks, strong, weak and rand password, random password, key loggers and spywares: s/w key loggers hardware key loggers, anti loggers, spywares, virus and worms, types of virus, Trojan horse and backdoors: backdoors, protection from Trojan horse, steganography, DoS and DDos attacks, SQL injection buffer overflow, attacks on wireless networks.

UNIT V:

Phishing and Identity theft: Introduction, phishing - methods of phishing, phishing techniques, spear phishing, types of phishing scams, phishing toolkit and spy phishing, phishing counter measures, Identity theft (ID theft) - Personally Identifiable Information (PII), types of identity theft, techniques of ID theft, Identity theft: counter measures, how to efface your Identity.

UNIT VI:

Cybercrime AND Cyber-security: The legal perspectives - Introduction, cybercrime and the legal landscape around the world, why do we need cyber laws: Indian context, The Indian Act, challenges of Indian law and cyber crime scenario in India, consequences of not adverting the weakness in Information Technology ACT, digital signature and the Indian ACT, Amendments to the Indian ACT, cybercrime and punishment, cyber laws, technology and student: Indian Scenario.

Text Books:

1. Naina Godbole, Sunil Belapure, "Cyber Security - Understanding Cybercrime, Computer forensic and legal perspective", Wiley India Pvt. Ltd.

Reference Books:

1. Thomas J. Mowbray, "Cyber security Managing systems- Conducting, Testing and Investigating Intrusion", Wiley

******