FTK-Centre for Information Technology

Cyber Security & Safety

Course Category:	**Skill Enhancement**
Credits:	**04** L-T-P: (2-1-1)
Target Semester:	The course will be offered to the pre-final & final year students of PG programs. If required, it may also be opted by Ph.D. students as one of the courses during the Ph.D. course work.
Maximum Intake:	**40**
Selection: Methodology:	**First-cum-first-serve basis**
Mode:	**Face-to-Face**

Objectives: The objective of this course is to introduce the students to the concepts of Cyber Security and Safety. The course will help students understand the necessary technical background required to understand Cyber Security and Safety measures. The knowledge acquired by the students would help them understand the typical modus-operandi of cybercriminals and counter techniques for safeguarding themselves and surrounding ecosystem by detecting, responding to, and preventing cybercrimes, cyberattacks & network intrusions. The course would also help students understand various provisions of IT Act 2000.

UNIT-I: Computer Network & Information Security

Introduction to Computer Networks & Network Protocols; Information Security vs Cyber Security; Expectations from Information Security; CIA Triad; Cyber Crimes; Internet; Introduction to Computer Networks & Network Protocols; Cyber Threats, Need for a Comprehensive Cyber Security Policy, Vulnerabilities-Overview, Cyber Assurance, Cyber Security Safeguards- Overview, Access control, Audit, Authentication, Biometrics, Cryptography, Deception, Denial of Service Filters, Ethical Hacking, Firewalls, Intrusion Detection Systems, Response, Scanning, Cyber Auditing/Assurance, Security policy, Threat Management; Google Dorks – Security implications, Cyber Kill Chain.

UNIT II: Cyber Crimes and safety

Introduction to cybercrimes, Kinds of cybercrimes: phishing, identify theft, cyberstalking, cyber terrorism, cyber obscenity, computer vandalism, Ransomware, Identity Theft, Forgery and fraud from Mobile Devices, Cyber risk associated with varied online activities and protection therefrom, Malware threats; Malware Kinds; Work on different digital platforms safely – Site certificates, malicious scripts, Online cybercrimes against women and impersonation scams, Security awareness on Wearable gadgets, Safety in Online Financial transactions

Concept and use of Cyber Hygiene in daily life, Browser Security, Wi-Fi Security, UPI Security, Juice Jacking, Google Map Security, OTP fraud, IOT Security, E-mails.

UNIT IV: Legal Perspective of Cyber Security

Concepts as defined in IT Act, Communication Device, Computer, Cyber Security, Data Security, Secure System, Online Gaming and its risks, Computer Fraud and Abuse Act, The Digital Millennium Copyright Act, IPR, Copyright Laws in India, Plagiarism, Basic concepts of Blockchain and Cryptocurrency. Cyber Security Standards. Reporting of Cybercrimes, Introduction to Cyber Forensics.

UNIT IV: Cyber Security in Practice

Introduction to E-Commerce & E-Business; Concept of E payments, ATM and Telebanking, Immediate Payment Systems, Mobile Money Transfer and E-Wallets, Unified Payment Interface, Cybercrimes in Electronic Payments, Precautions in Electronics Money Transfer, RBI Guidelines of Customer Protection in Unauthorized Banking Transactions, KYC: Concept, cases, and safeguards

Social Network and its contents, blogs, Safe and Proper use of Social Networks, Inappropriate Content on Social Networks, Flagging and reporting of inappropriate content, Laws regarding posting of inappropriate content. Protecting reputation.

Suggested books:

- The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy. Netherlands: Elsevier Science. Cross, M., Sammons, J. (2016)
- Cyber Law 3.0: An Exhaustive Section Wise Commentary on The Information Technology Act Along with Rules, Regulations, Policies, Notifications Etc. India: Universal, LexisNexis. Duggal, P. (2018).
- Information Security & Cyber Laws. (n.d.). India: Khanna Book Publishing Company (P) Limited.