GUJARAT TECHNOLOGICAL UNIVERSITY
MASTER OF COMPUTER APPLICATIONS (MCA)
SEMESTER: V

Subject Name: **Cyber Security and Forensics (CSF) (Elective-II)**
Subject Code: **650008**

Objectives:

- To understand the major concepts of Cyber Security and Forensics and to create the awareness through simple practical tips and tricks and to educate the students to learn how to avoid becoming victims of cyber crimes.
- The subject and the course content will help to the student who wish to take up cyber forensics as career as well as those who want to seek careers in cyber security.
- To gain experience of doing independent study and research in the field of cyber security and cyber forensics.

Prerequisites:

Basic fundamental knowledge of Networking, Web Application, Mobile Application and Relational Database Management System

Contents:

UNIT- I: Introduction to Cybercrime: [10%]

Introduction, Cybercrime: Definition and Origins of the Word, Cybercrime and Information Security, Who are Cybercriminals? Classifications of Cybercrimes: E-Mail Spoofing, Spamming, Cyber defamation, Internet Time Theft, Salami Attack/Salami Technique, Data Diddling, Forgery, Web Jacking, Newsgroup Spam/Crimes Emanating from Usenet Newsgroup, Industrial Spying/Industrial Espionage, Hacking, Online Frauds, Pornographic Offenses , Software Piracy, Computer Sabotage, E-Mail Bombing/Mail Bombs, Usenet Newsgroup as the Source of Cybercrimes , Computer Network Intrusions, Password Sniffing, Credit Card Frauds, Identity Theft

UNIT- II: Cyberoffenses: How Criminals Plan Them [10%]

Introduction, Categories of Cybercrime, How Criminals Plan the Attacks: Reconnaissance, Passive Attack, Active Attacks, Scanning/Scrutinizing gathered Information, Attack (Gaining and Maintaining the System Access), Social Engineering, and Classification of Social Engineering, Cyberstalking: Types of Stalkers, Cases Reported on Cyberstalking, How Stalking Works? Real-Life Incident of Cyberstalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Botnet, Attack Vector Cloud Computing: Why Cloud Computing? , Types of Services, Cybercrime and Cloud Computing

UNIT- III: Cybercrime: Mobile and Wireless Devices [20%]

Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era: Types and Techniques of Credit Card Frauds, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices Authentication Service Security: Cryptographic Security for Mobile Devices, LDAP Security for Hand-Held Mobile Computing Devices, RAS Security for Mobile Devices, Media Player Control Security, Networking

API Security for Mobile Computing Applications, Attacks on Mobile/Cell Phones: Mobile Phone Theft, Mobile Viruses, Mishing, Vishing, Smishing, Hacking Bluetooth, Mobile Devices: Security Implications for Organizations: Managing Diversity and Proliferation of Hand-Held Devices, Unconventional/Stealth Storage Devices Threats through Lost and Stolen Devices, Protecting Data on Lost Devices, Educating the Laptop Users

Organizational Measures for Handling Mobile Devices-Related Security Issues: Encrypting Organizational Databases, Including Mobile Devices in Security Strategy, Organizational Security Policies and Measures in Mobile Computing Era: Importance of Security Policies relating to Mobile Computing Devices, Operating Guidelines for Implementing Mobile Device Security Policies, Organizational Policies for the Use of Mobile Hand-Held Devices, Laptops: Physical Security Countermeasures

UNIT- IV: Tools and Methods Used in Cybercrime [15%]

Introduction, Proxy Servers and Anonymizers, Phishing: How Phishing Works? Password Cracking: Online Attacks, Offline Attacks, Strong, Weak and Random Passwords, Random Passwords, Keyloggers and Spywares: Software Keyloggers, Hardware Keyloggers, Antikeylogger, Spywares, Virus and Worms: Types of Viruses, Trojan Horses and Backdoors: Backdoor, How to Protect from Trojan Horses and Backdoors, Steganography: Steganalysis, DoS and DDoS Attacks: DoS Attacks, Classification of DoS Attacks, Types or Levels of DoS Attacks, Tools Used to Launch DoS Attack, DDoS Attacks, How to Protect from DoS/DDoS Attacks, SQL Injection: Steps for SQL Injection Attack, How to Avoid SQL Injection Attacks, Buffer Overflow: Types of Buffer Overflow, How to Minimize Buffer Overflow, Attacks on Wireless Networks: Traditional Techniques of Attacks on Wireless Networks, Theft of Internet Hours and Wi-Fi-based Frauds and Misuses, How to Secure the Wireless Networks

UNIT- V: Phishing and Identity Theft [5%]

Introduction, Phishing: Methods of Phishing, Phishing Techniques, Spear Phishing, Types of Phishing Scams, Phishing Toolkits and Spy Phishing, Phishing Countermeasures, Identity Theft (ID Theft): Personally Identifiable Information(PII), Types of Identity Theft, Techniques of ID Theft, Identity Theft-Countermeasures, How to Protect your Online Identity

UNIT- VI: Cybercrimes and Cybersecurity: The Legal Perspectives [15%]

Introduction, Why Do We Need Cyberlaws: The Indian Context, The Indian IT Act: Admissibility of Electronic Records: Amendments made in the Indian ITA 2000, Positive Aspects of the ITA 2000, The Weak Areas of the ITA 2000, Challenges to Indian Law and Cybercrime Scenario in India, Consequences of Not Addressing the Weakness in Information Technology Act
Amendments to the Indian ITA 2008: Overview of Changes Made to the Indian IT Act, Cybercafe-Related Matters Addressed in the Amendment to the Indian IT Act, State Government Powers Impacted by the Amendments to the Indian IT Act, Impact of IT Act Amendments Impact Information Technology Organizations, Cybercrime and Punishment, Cyberlaw, Technology and Students: Indian Scenario

UNIT- VII: Understanding Computer Forensics [20%]

Introduction, Historical Background of Cyberforensics, Digital Forensics Science, The Need for Computer Forensics, Cyberforensics and Digital Evidence: The Rules of Evidence,Forensics Analysis of E-Mail: RFC282, Digital Forensics Life Cycle: The Digital Forensics Process,The Phases in Computer Forensics/Digital Forensics, Precautions to be Taken when Collecting Electronic Evidence, Chain of Custody Concept, Network Forensics, Approaching a Computer Forensics Investigation: Typical Elements Addressed in a Forensics Investigation Engagement Contract, Solving a Computer Forensics Case, Setting up a Computer Forensics Laboratory: Understanding the Requirements, Computer Forensics and Steganography: Rootkits, Information Hiding, Relevance of the OSI 7 Layer Model to Computer Forensics: Step 1: Foot Printing, Step 2: Scanning and Probing, Step 3: Gaining Access, Step 4: Privilege, Step 5: Exploit, Step 6: Retracting, Step 7: Installing Backdoors,

Forensics and Social Networking Sites: The Security/Privacy Threats, Challenges in Computer Forensics: Technical Challenges: Understanding the Raw Data and its Structure, The Legal Challenges in Computer Forensics and Data Privacy Issues, Special Tools and Techniques: Digital Forensics Tools Ready Reckenor, Special Technique: Data Mining used in Cyberforensics, Forensics Auditing, Antiforensics

UNIT- VIII: Forensics of Hand-Held Devices [5%]

Introduction, Hand-Held Devices and Digital Forensics: Mobile Phone Forensics, PDA Forensics, Printer Forensics, Scanner Forensics, Smartphone Forensics, iPhone Forensics, Challenges in Forensics of the Digital Images/Still Camera, Forensics of the BlackBerry Wireless Device, Toolkits for Hand-Held Device Forensics: EnCase, Device Seizure and PDA Seizure, Palm DD, Forensics Card Reader, Cell Seizure, MOBILedit!, ForensicSIM, Organizational Guidelines on Cell Phone Forensics: Hand-Held Forensics as the Specialty Domain in Crime Context

Cybercrime: Illustrations, Examples and Mini-Cases, Scams
(Only for the referential context should not be asked in the examination)

Real-Life Examples
- Example 1: Official Website of Maharashtra Government Hacked
- Example 2: E-Mail Spoofing Instances
- Example 3: I Love You Melissa – Come Meet Me on the Internet
- Example 4: Ring-Ring Telephone Ring: Chatting Sessions Turn Dangerous
- Example 5: Young Lady's Privacy Impacted
- Example 6: Indian Banks Lose Millions of Rupees
- Example 7: "Justice" vs. "Justice": Software Developer Arrested for Launching Website Attacks
- Example 8: Parliament Attack
- Example9: Pune City Police Bust Nigerian Racket

Mini-Cases:
- Mini-Case 1: Cyberpornography Involving a Juvenile Criminal
- Mini-Case 2: Cyberdefamation: A Young Couple Impacted
- Mini-Case 12: Internet Used for Murdering
- Mini-Case 13: Social Networking Victim – The MySpace Suicide Case
- Mini-Case 16: NASSCOM vs. Ajay Sood and Others

Online Scams:
- Scam No. 1 – Foreign Country Visit Bait
- Scam No. 2 – Romance Scam
- Scam No. 3 – Lottery Scam
- Scam No. 4 – Bomb Scams
- Scam No. 5 – Charity Scams
- Scam No. 6 – Fake Job Offer Scam

Financial Crimes in Cyber Domain:
- Financial Crime 1: Banking Related Frauds
- Financial Crime 2: Credit Card Related Frauds

Text Book:

1. Nina Godbole, Sunit Belapur, "Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley India Publications, April, 2011

Reference Books:

1. Robert Jones, “Internet Forensics: Using Digital Evidence to Solve Computer Crime”, O’Reilly Media, October, 2005
2. Chad Steel, “Windows Forensics: The field guide for conducting corporate computer investigations”, Wiley India Publications, December, 2006

Chapter wise Coverage from the Text Book:

Reference Book: 1

Chapter 1: 1.1 to 1.5
Chapter 2: 2.1 to 2.8
Chapter 3: 3.1 to 3.12
Chapter 4: 4.1 to 4.12
Chapter 5: 5.1, 5.2, 5.3
Chapter 6: 6.1, 6.3, 6.4, 6.5, 6.6, 6.8, 6.9, 6.10
Chapter 7: 7.1 to 7.14, 7.16, 7.17, 7.18, 7.19
Chapter 8: 8.1, 8.3, 8.4, 8.8