



## **C. U. SHAH UNIVERSITY – WADHWAN CITY**

### **FACULTY OF TECHNOLOGY AND ENGINEERING DEPARTMENT OF COMPUTER ENGINEERING M. TECH. SEMESTER: - III**

**SUBJECT NAME: Cyber Security Standards (CSS)**

**SUBJECT CODE: 5TE03CSS1**

**Teaching & Evaluation Scheme: -**

Subject Code	Subject Name	Teaching Scheme (Hours)				Credits	Evaluation Scheme							
		Th	Tu	Pr	Total		Theory				Practical (Marks)			Total
							Sessional Exam		University Exam		Internal		University	
							Marks	Hours	Marks	Hours	Pr/Viva	TW	Pr	
5TE03CSS1	Cyber Security Standards	4	0	2	6	5	30	1.5	70	3.0	-	20	30	150

#### **Objectives:**

- To understand the concepts of cyber security Attacks, Tools and Preventions.

#### **Prerequisites:**

- Knowledge of Computer Network, Information security and wide knowledge of internet.

#### **Course outline:**

Sr. No.	Course Contents
1	Introduction · Cybercrime: Cybercrime and Information Security · Who are Cybercriminals? · Classifications of Cybercrimes · Cybercrime: The Legal Perspectives · Cybercrimes: An Indian Perspective.
2	Cyberoffenses: How Criminals Plan Them · How Criminals Plan the Attacks · Social Engineering · Cyberstalking · Cybercafe and Cybercrimes · Botnets: The Fuel for Cybercrime · Attack Vector · Cloud Computing
3	Cybercrime: Mobile and Wireless Devices · Proliferation of Mobile and Wireless Devices · Trends in Mobility · Credit Card Frauds in Mobile and Wireless Computing Era · Security Challenges Posed by Mobile Devices · Registry Settings for Mobile Devices · Authentication Service Security · Attacks on Mobile/Cell Phones · Mobile Devices: Security Implications for Organizations.
4	Tools and Methods Used in Cybercrime · Introduction · Proxy Servers and Anonymizers · Phishing · Password Cracking · Keyloggers and Spywares · Virus and Worms · Trojan Horses and Backdoors · Steganography · DoS and DDoS Attacks · SQL Injection · Buffer Overflow · Attacks on Wireless Networks
5	Phishing and Identity Theft · Introduction · Phishing · Identity Theft (ID Theft)
6	Cybercrimes and Cybersecurity: The Legal Perspectives · Introduction · Cybercrime and the Legal Landscape around the World · Why Do We Need Cyberlaws: The Indian Context · The Indian IT Act · Challenges to Indian Law and Cybercrime Scenario in India · Consequences of Not Addressing the

	Weakness in Information Technology Act · Digital Signatures and the Indian IT Act · Amendments to the Indian IT Act · Cybercrime and Punishment.
7	Understanding Computer Forensics · Introduction · Historical Background of Cyberforensics · Digital Forensics Science · The Need for Computer Forensics · Cyberforensics and Digital Evidence · Forensics Analysis of E-Mail · Digital Forensics Life Cycle · Chain of Custody Concept · Network Forensics · Approaching a Computer Forensics Investigation · Setting up a Computer Forensics Laboratory: Understanding the Requirements · Computer Forensics and Steganography · Relevance of the OSI 7 Layer Model to Computer Forensics · Forensics and Social Networking Sites: The Security/Privacy Threats · Computer Forensics from Compliance Perspective · Challenges in Computer Forensics · Special Tools and Techniques · Forensics Auditing · Antiforensics
8	Cybercrimes Case study

### Learning Outcomes:

At the end of this module the student should be well familiar with:

- It provides the much needed awareness in the times of growing cybercrimes.
- It provides adequate orientation on laws in reference to cybercrime and cyber security taking into account the Indian as well as global scenario.

### Books Recommended:

1. Cyber security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by **Nina Godbole, Sunit Belapure**, Wiley (2011).
2. security in computing, 4th Edition by **Charles P. Pfleegar and shari lawrence Pfleegar**, Pearson (2009).
3. Cyber security Operations handbook by **John W. Rittinghouse and william N hancock**, Digital Press (2003).
4. Software Forensics by **Robert M. Slade**, Tata Mcgraw-Hill (2005).