A Six Months Course

on

CYBER SECURITY

DETAILED COURSE STRUCTURE

Cybersecurity Fundamentals

E-Commerce and Digital Security

Cyber Laws and Security Management

Course Coordinator:

Dr. B. Sateesh Kumar

Professor & Head,

Department of CSE,

JNTUH University College of Engineering Jagtial.

STRUCTURE OF CYBER SECURITY COURSE

SUBJECT NAME	CYBERSECURITY FUNDAMENTALS
SESSION-1	**INTRODUCTION TO CYBERSECURITY**
DAY-1	**Understanding Cyberspace** Defining Cyberspace and Overview of Computer and Web Technology, Architecture of Cyberspace
DAY-2	**Internet Technology** Communication and Web Technology, Internet, World Wide Web, Advent of the Internet
DAY-3	**Regulation and Governance of Cyberspace** Regulation of Cyberspace, Internet Infrastructure for Data Transfer and Governance, Internet Society
DAY-4	**Cybersecurity Fundamentals and Challenges** Concept of Cybersecurity, Issues and Challenges of Cybersecurity
SESSION-2	**CYBER-ATTACKS OVERVIEW**
DAY-5	**Basics of Cybersecurity Attacks** Need for Cybersecurity, Introduction to Cyber Attacks, Classification of Cyberattacks, Classification of Malware, Threats
DAY-6	**Security Models and Mechanisms** Different Security Models and Security Mechanisms, Information Security and Network Security
DAY-7	**Intrusion Detection and Prevention** Intrusion Detection Systems, Intrusion Prevention Systems
SESSION-3	**CYBER CRIMES & CYBER LAWS**
DAY-8	**Types of Cybercrime and Prevention** Classification of Cybercrimes, Common Cybercrimes - Cybercrime Targeting Computers and Mobiles, Cybercrime Against Women and Children, Financial Frauds, Social Engineering Attacks, Malware and Ransomware Attacks, Zero-Day and Zero-Click Attacks, Cyber Criminals' Modus Operandi, Reporting of Cybercrimes, Remedial and Mitigation Measures
DAY-9	**Legal Aspects and Regulations** The Legal Perspective of Cybercrime, IT Act 2000 and Its Amendments, Cybercrime and Offences, Organizations Dealing with Cybercrime and Cybersecurity in India
DAY-10	**Case Studies and Practical Application** Case Studies
SESSION-4	**SECURITY ESSENTIALS**
DAY-11	**Web Browser Security:** Securing web browser, Two-step Authentication
DAY-12	**Password Security:** Guidelines for setting up a secure password, Security Guidelines for Point of Sales (POS)

DAY-13 **Mobile Security:**
Wi-Fi Security, Smartphone Security, Android Security, Online Banking Security, Mobile Banking Security, Security of Debit and Credit Cards, UPI Security, E-wallet Security

SESSION-5 **SOCIAL MEDIA SECURITY-1**

DAY-14 **Social Media Basics:**
Introduction to Social networks, Types of Social media, Social media platforms

DAY-15 **Social Media Engagement and Strategy:**
Hashtag, Viral content, Social media marketing, Social media monitoring

DAY-16 **Social Media Concerns and Considerations:**
Social media privacy, Challenges, opportunities, and pitfalls in online social networks

SESSION-6 **SOCIAL MEDIA SECURITY-2**

DAY-17 **Security and Content Control:**
Security issues related to social media, Flagging and reporting of inappropriate content, Laws regarding posting of inappropriate content

DAY-18 **Best Practices and Responsible Usage:**
Best practices for the use of social media

DAY-19 **Illustrative Examples:**
Case studies

PRACTICAL SESSION-1

DAY-20 1. Checklist for reporting cyber crime at Cyber crime Police Station.

DAY-21 2. Checklist for reporting cyber crime online.

DAY-22 3. Reporting phishing emails.
4. Demonstration of email phishing attack and preventive measures.

PRACTICAL SESSION-2

DAY-23 1. Basic checklist, privacy and security settings for popular Social media platforms.

DAY-24 2. Reporting and redressal mechanism for violations and misuse of Social media platforms.

STRUCTURE OF CYBER SECURITY COURSE

SUBJECT NAME	*E-COMMERCE & DIGITAL SECURITY*
SESSION-1	**E-COMMERCE**
DAY-1	**E-Commerce Fundamentals:** Definition of E-Commerce, Main components of E-Commerce
DAY-2	**E-Commerce Security:** Elements of E-Commerce security, E-Commerce threats, E-Commerce security best practices
SESSION-2	**DIGITAL PAYMENTS**
DAY-3	**Digital Payment Fundamentals:** Introduction to digital payments, Components of digital payment and stakeholders
DAY-4	**Modes of Digital Payments and Security:** Modes of digital payments (Banking Cards, UPI, e-Wallets, USSD, Aadhar enabled payments), Digital payments related common frauds and preventive measures
DAY-5	**Legal and Regulatory Framework:** RBI guidelines on digital payments and customer protection in unauthorized banking transactions, Relevant provisions of Payment Settlement Act, 2007
SESSION-3	**DIGITAL DEVICES SECURITY**
DAY-6	**Device and Mobile Security:** End Point device and Mobile phone security, Password policy, Security patch management, Data backup, Downloading and management of third-party software, Device security policy
DAY-7	**Tools and Technologies for Cyber Security:** Authentication tools, firewalls, intrusion detection systems, and antivirus and encryption software.
DAY-8	**Cyber Security Best Practices:** Cyber Security best practices, Significance of host firewall and Anti-virus, Management of host firewall and Anti-virus, Wi-Fi security, Configuration of basic security policy and permissions
SESSION-4	**CYBER SECURITY LANDSCAPE**
DAY-9	**Cyber Threat Landscape and Terminology:** Cyber security increasing threat landscape, Cyber security terminologies (Cyberspace, attack, attack vector, attack surface, threat, risk, vulnerability, exploit, exploitation, hacker), Non-state actors, Cyber terrorism
DAY-10	**Protection and Security Measures:** Protection of end-user machines, Critical IT and National Critical Infrastructure, Cyberwarfare
DAY-11	**Practical Insights and Examples:** Case Studies

SESSION-5	CYBER CRIMES
DAY-12	**Cyber Crimes Targeting Computer Systems and Mobile Devices:** Data diddling attacks, Spyware, Logic bombs, DoS (Denial of Service), DDoS (Distributed Denial of Service), APTs (Advanced Persistent Threats), Viruses, Trojans, Ransomware, Data breach
DAY-13	**Online Scams and Frauds:** Email scams, Phishing, Vishing, Smishing, Online job fraud, Online sextortion, Debit/credit card fraud, Online payment fraud
DAY-14	**Cyberbullying and Web Exploitation:** Cyberbullying, Website defacement, Cybersquatting, Pharming
DAY-15	**Darknet and Illicit Activities:** Cyber espionage, Crypto-jacking, Darknet activities, including illegal trades, drug trafficking, and human trafficking
SESSION-6	SOCIAL MEDIA SECURITY
DAY-16	**Social Media Scams, Frauds, and Cyber Crimes:** Impersonation, Identity theft, Job scams, Misinformation and fake news
DAY-17	**Cyber Crimes Against Persons and Social Engineering:** Cyber grooming, Child pornography, Cyber stalking, Social Engineering attacks
DAY-18	**Law Enforcement and Reporting:** Cyber Police stations, Crime reporting procedure, Case studies
PRACTICAL SESSION-1	
DAY-19	1. Configuring security settings in Mobile Wallets and UPIs. 2. Checklist for secure net banking.
DAY-20	3. Setting, configuring and managing three password policy in the computer (BIOS, Administrator and Standard User). 4. Setting and configuring two factor authentication in the Mobile phone.
DAY-21	5. Security patch management and updates in Computer and Mobiles. 6. Managing Application permissions in Mobile phone.
PRACTICAL SESSION-2	
DAY-22	1. Installation and configuration of computer Anti-virus.
	2. Installation and configuration of Computer Host Firewall.
DAY-23	3. Wi-Fi security management in computer and mobiles for reporting cyber-crimes.
DAY-24	4. Checklist for reporting cyber-crimes online

STRUCTURE OF CYBER SECURITY COURSE

SUBJECT NAME	CYBER LAW & SECURITY MANAGEMENT
SESSION-1	**CYBER LAWS-1**
DAY-1	**Cybercrime and Legal Landscape Around the World:** Introduction Cybercrime and Legal Landscape Around the World
DAY-2	**IT Act Amendments and Limitations:** IT Act, 2000 and its amendments. Limitations of IT Act, 2000. Cybercrime and punishments.
SESSION-2	**CYBER LAWS-2**
DAY-3	**Cyber Laws and Legal and Ethical Aspects Related to New Technologies:** Legal and ethical aspects related to new technologies - AI/ML, IoT, Blockchain, Darknet, and Social media.
DAY-4	**Cyber Laws of Other Countries** Cyber Laws of other countries – Importance and Examples.
DAY-5	**Case Studies:** Case Studies on Cyber Laws and their Execution.
SESSION-3	**DATA PRIVACY AND DATA SECURITY -1**
DAY-6	**Data Definitions and Data Protection:** Defining data, meta-data, big data, and nonpersonal data. Data protection, data privacy, and data security.
DAY-7	**Legal Framework and Compliance:** Personal Data Protection Bill and its compliance. Data protection principles.
DAY-8	**Challenges and Issues with Big Data:** Big data security issues and challenges.
SESSION-4	**DATA PRIVACY AND DATA SECURITY -2**
DAY-9	**Data Protection Regulations of Other Countries:** General Data Protection Regulation (GDPR), 2016. Personal Information Protection and Electronic Documents Act (PIPEDA).
DAY-10	**Social Media Data Privacy and Security:** Social media data privacy and security issues.
DAY-11	
SESSION-5	**CYBER SECURITY MANAGEMENT**
DAY-12	**Cybersecurity Policies and Planning:** Cybersecurity Plan, Cybersecurity Policy, Cyber Crisis Management Plan
DAY-13	**Business Continuity and Risk Assessment:** Business Continuity, Risk Assessment, Examples.

DAY-14	**Security Controls and Goals:** Types of Security Controls, Goals of Security Controls
DAY-15	
SESSION-6	**CYBER SECURITY COMPLIANCE AND GOVERNANCE**
DAY-16	**Cyber security audit and compliance:**
DAY-17	**National cyber security policy and strategy:**
DAY-18	
PRACTICAL SESSION-1	
DAY-19	1. Configuring security settings in Mobile Wallets and UPIs. 2. Checklist for secure net banking.
DAY-20	3. Setting, configuring and managing three password policy in the computer (BIOS, Administrator and Standard User). 4. Setting and configuring two factor authentication in the Mobile phone.
DAY-21	5. Security patch management and updates in Computer and Mobiles.
DAY-22	6. Managing Application permissions in Mobile phone.
PRACTICAL SESSION-2	
DAY-23	1. Installation and configuration of computer Anti-virus.
	2. Installation and configuration of Computer Host Firewall.
DAY-24	3. Wi-Fi security management in computer and mobiles for reporting cyber-crimes. 4. Checklist for reporting cyber-crimes online

References:

1. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd.

2. Information Warfare and Security by Dorothy F. Denning, Addison Wesley.

3. Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform.

4. Data Privacy Principles and Practice by Natraj Venkataramanan and Ashwin Shriram, CRC Press.

5. Information Security Governance, Guidance for Information Security Managers by W. Krag Brothy, 1st Edition, Wiley Publication.

6. Auditing IT Infrastructures for Compliance By Martin Weiss, Michael G. Solomon, 2nd Edition, Jones Bartlett Learning.

7. "Cybersecurity and Cyberwar: What Everyone Needs to Know" by P.W. Singer and Allan Friedman, 1st Edition, Oxford University Press.

8. "Applied Cryptography" by Bruce Schneier, 2nd Edition, Wiley.

9. "The Web Application Hacker's Handbook" by Dafydd Stuttard and Marcus Pinto, 2nd Edition, Wiley.

10. "Hacking Exposed" by Stuart McClure, Joel Scambray, and George Kurtz, 7th Edition, McGraw-Hill Education