Syllabus

Module 1: Introduction to Cybersecurity (साइबर सुरक्षा का परिचय)

a. Intro to Cyber Security (साइबर सुरक्षा का परिचय)

i. Basic security concepts: Confidentiality, Integrity, Availability

(बुनियादी सुरक्षा अवधारणाएं : गोपनीयता, अखंडता, उपलब्धता)

ii. Importance of Cyber security (साइबर सुरक्षा का महत्व)

b. Cyber Security vs. Cyber Crime (साइबर सुरक्षा बनाम साइबर अपराध)

i. Types of modern Cyber threats: malware, phishing, MITM attacks, Dos/DDoS

(आधुनिक साइबर खतरों के प्रकार: मैलवेयर, फ़िशिंग, मैन इन द मिडिल अटैक, डिनायल ऑफ़ सर्विस/डिस्ट्रिब्यूटेड डिनायल ऑफ़ सर्विस अटैक)

c. Introduction to MITRE TTPs and Cyber Kill Chain

(MITRE TTPs एवं साइबर किल चेन का परिचय)

d. Discussion on real-world cyber attacks

(वास्तविक दुनिया के साइबर हमलों पर चर्चा)

i. Some real-world Cyber Fraud and Cyber Crime Cases

(वास्तविक दुनिया के कुछ साइबर धोखाधड़ी व् साइबर अपराध के मामले)

Module 2: Cyber Threat Landscape (साइबर खतरा परिदृश्य)

a. Types of Malware: Viruses, Worms, Trojans, Ransomware

(मैलवेयर के प्रकार: वाइरस, ट्रोजन्स, वर्म्स, ट्रोजन्स, रैंसमवैर)

b. Phishing Attacks: Techniques and Prevention

(फिशिंग हमले : तकनीक व् रोकथाम)

c. Social Engineering: Recognizing and Responding to Social Engineering Attempts

(सोशल इंजीनियरिंग : सोशल इंजीनियरिंग प्रयासों को पहचानना व् उनका जवाब देना)

d. Various Cyber Fraud/Cyber Crime Methods

(विभिन्न साइबर धोखाधड़ी/साइबर अपराध के तरीके)

i. OTP fraud, Deepfake based Frauds, Voice Cloning, Cyber Bullying, Cyber Extortion

(OTP धोखाधड़ी , डीपफेक आधारित धोखाधड़ी , वॉयस क्लोनिंग, साइबर बुलिंग, साइबर एक्सटॉर्शन)

ii. Various Cyber Crime Reporting numbers and websites.

(OTP धोखाधड़ी , डीपफेक आधारित धोखाधड़ी , वॉयस क्लोनिंग, साइबर बुलिंग, साइबर एक्सटॉर्शन)

e. Cyber warfare concept and concerns

(साइबर युद्ध की अवधारणा व् चिंता)

f. Outlines of IT Act 2008, and DPDP Act 2023

(IT एक्ट 2008 व् DPDP एक्ट 2023 की रुपरेखा)

Module 3: Data Protection and Encryption (डाटा सुरक्षा व् एन्क्रिप्शन)

a. Importance of Data Backup and Recovery (डाटा बैकअप व् रिकवरी का महत्त्व)

b. Data Encryption: Understanding Encryption Techniques

(डाटा एन्क्रिप्शन : एन्क्रिप्शन तकनीकों को समझना)

c. Securing Online Transactions and Financial Information

(ऑनलाइन लेन देन व् वित्तीय जानकारी को सुरक्षित करना/रखना)

Module 4: Securing Digital Devices and Networks

(डिजिटल उपकरणों और नेटवर्क को सुरक्षित रखना)

a. Device Security: Protecting Computers, Smartphones, and Tablets

(डिवाइस सुरक्षा: कंप्यूटर, स्मार्ट फ़ोन और टेबलेट्स की सुरक्षा करना)

b. Network Security Basics: Wi-Fi Security, Firewalls, etc.

(नेटवर्क सुरक्षा की मूल बातें : वाई फाई सुरक्षा, फायरवॉल इत्यादि)

c. Secure Web Browsing Practices

(सुरक्षित वेब ब्राउज़िंग प्रथाएं)

d. Understanding https, SSL certificate, Creating your own SSL certificates and its limitations, the need for PKI

(https, SSL certificate को समझना , अपना स्वयं का SSL certificates बनाना एवं इसकी सीमाओं को समझना ,PKI की आवश्यकता)

Module 5: Application security (एप्लीकेशन सुरक्षा)

a. Secure coding principles (सुरक्षित कोडिंग सिद्धांत)

b. Common coding vulnerabilities: SQL Injection, XXS, CSRF etc.

(सामान्य कोडिंग कमज़ोरियाँ : SQL इंजेक्शन, क्रॉस साइट स्क्रिप्टिंग, CSRF इत्यादि)

c. Intro to OWASP Top 10, Burp Suite

(OWASP Top 10, Burp Suite का परिचय)

Module 6: OS protection Fundamentals (ऑपरेटिंग सिस्टम सुरक्षा)

a. Understanding User accounts (Linux and Windows)

(यूजर एकाउंट्स को समझना (लिनक्स एवं विंडोज))

b. File and Directory Permissions (फाइल एवं डायरेक्टरी की अनुमतियाँ)

c. Antivirus and it's usage. (एंटी वायरस एवं उसका उपयोग)

d. Application and Execution Control (आवेदन एवं निष्पादन नियंत्रण)

e. Update and Patching (अपडेट एवं पैचिंग)

f. Understanding threats to DNS hijacking, DNS poisoning and problem of using public Wi-Fi or public open networks

(DNS hijacking, DNS poisoning और सार्वजानिक वाई फाई व् सार्वजनिक खुले नेटवर्क का उपयोग करने की समस्या के खतरों को समझना)