Format for the Syllabus of Vocational Course

Paper Name – Cyber Security Vocational Course **VOC160**

Paper Code –

Course Objectives – This course explores the most critical elements of cybersecurity. It covers systems, applications, networks, cryptography, and OS security. This fully online course provides students with fundamental knowledge and hands-on experience in cybersecurity. An integral part of the program is the customized labs, which will be provided at every student's desk through our virtual labs.

Course Content –

1. Introduction to Cybersecurity
    a. Intro to Cyber Security
        i. Basic security concepts: Confidentiality, Integrity, Availability
        ii. Importance of Cyber security
    b. Cyber Security vs. Cyber Crime
        i. Types of modern Cyber threats: malware, phishing, MITM attacks, Dos/DDoS
    c. Introduction to MITRE TTPs and Cyber Kill Chain
    d. Discussion on real-world cyber attacks
        i. Some real-world Cyber Fraud and Cyber Crime Cases
2. Cyber Threat Landscape
    a. Types of Malware: Viruses, Worms, Trojans, Ransomware
    b. Phishing Attacks: Techniques and Prevention
    c. Social Engineering: Recognizing and Responding to Social Engineering Attempts
    d. Various Cyber Fraud/Cyber Crime Methods
        i. OTP fraud, Deepfake based Frauds, Voice Cloning, Cyber Bullying, Cyber Extortion
        ii. Various Cyber Crime Reporting numbers and websites.
    e. Cyber warfare concept and concerns
    f. Outlines of IT Act 2008, and DPDP Act 2023
3. Data Protection and Encryption
    a. Importance of Data Backup and Recovery
    b. Data Encryption: Understanding Encryption Techniques
    c. Securing Online Transactions and Financial Information
4. Securing Digital Devices and Networks
    a. Device Security: Protecting Computers, Smartphones, and Tablets
    b. Network Security Basics: Wi-Fi Security, Firewalls, etc.
    c. Secure Web Browsing Practices

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

5. Application security
    a. Secure coding principles
    b. Common coding vulnerabilities: SQL Injection, XXS, CSRF etc.
    c. Intro to OWASP Top 10, Burp Suite
6. OS protection Fundamentals
    a. Understanding User accounts (Linux and Windows)
    b. File and Directory Permissions
    c. Antivirus and it's usage.
    d. Application and Execution Control
    e. Update and Patching
    f. Understanding threats to DNS hijacking, DNS poisoning and problem of using public Wi-Fi or public open networks

Total weightage of Theory - 40% of marks, 15 hours (1 Credit)

Total weightage of Practical - 60% of marks, 30 hours (Lecture for conducting practical sessions) + 30 hours (Virtual Labs for students for hands-on experience) (2 Credit)

Practicum Work - At least 4 activities should be given. Two activities will be selected by the students for their assessment of Practicum Work

Practical sessions will be in conjunction with the above modules. Some sample sessions –

1. Understanding packet capturing and understanding use of Wireshark
2. Understanding File Permissions in Linux and in Windows
3. Understanding creating public/private keypair, creating a digital certificate, analyzing digital certificates of websites
4. Examples of Buffer overflow
5. Example examples of privilege escalation to obtain a root shell.
6. DVWA based web security exercises.
7. Example on ARP protocol and ARP poisoning
8. Example on setting up Firewall on Linux and Windows

Learning Outcomes –

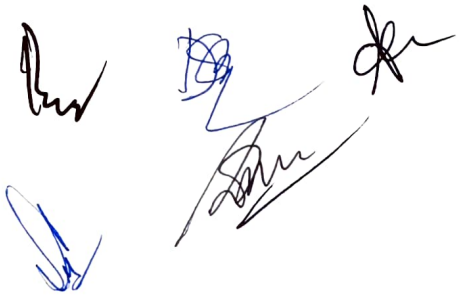
- Introduces real-time cybersecurity techniques and methods within the context of protocol suites, highlighting the necessity for network security solutions.
- Deepens understanding of the technical foundations of cyberspace and related cyber issues.
- Equips learners with foundational knowledge of common cybersecurity threats, vulnerabilities, and risks.

- Teaches the configuration and management of essential security tools such as firewalls, intrusion detection systems (IDS), and antivirus software to protect systems from malicious attacks.
- Encourages ongoing professional development and staying current with evolving cybersecurity trends and best practices through certifications, training programs, and participation in cybersecurity communities.

Job Prospects –

Skill Partner –

Suggested Reading –



Cybersecurity Vocational Course

A walk through with the details of the program

Cybersecurity Vocational Course Modules

Module Names		Module Names
Cyber Crime and Cyber Hygiene	5:30 Hours	
Social Media Threats and Cyberbullying	5:30 Hours	
Identity Theft and Personal Data Leaks	5:30 Hours	
Online Financial Frauds and Digital Payments Security	5:30 Hours	
Women and Child Online Safety	5:30 Hours	
Awareness on Ransomware	3:00 Hours	
Dark Web, Cyber Terrorism & Illegal Activities	5:30 Hours	
Best Practices for Cyber Hygiene	5:30 Hours	

Cybersecurity Vocational Course Objectives

- **Spot Common Online Dangers -** Learn to recognize threats like ransomware (files held for ransom), spyware (secret monitoring), identity theft, and cyberbullying.

- **Protect Your Personal Information -** Understand how to keep your name, address, photos, and bank details safe from misuse.

- **Practice Simple Cyber Hygiene -** Use strong, unique passwords; turn on two-step verification; install updates; and back up important files regularly.

- **Conduct Safe Online Transactions -** Check website addresses, use trusted payment apps, and watch for phishing messages before sending money.

- **Understand the "Hidden" Internet -** Gain a basic idea of the dark web, why some activities there are illegal, and how to report suspicious sites or content.

Cybersecurity Vocational Course Learning Outcomes

❖ Define common cyber threats (ransomware, spyware, phishing, identity theft, cyberbullying)

❖ Identify risks in everyday activities—such as social media use, online shopping, and digital payments—by spotting fake links, suspicious messages, or unsecured websites.

❖ Demonstrate basic cyber hygiene: create strong, unique passwords; enable two-step verification; install software updates; and back up important files.

❖ Apply safe transaction practices: verify website URLs, use trusted payment apps, and recognize phishing attempts before sharing financial information.

Cybersecurity Vocational Course Learning Outcomes

❖ Explain how to protect personal data (name, address, photos, bank details) and decide when and what to share online.

❖ Recognize signs of illegal activity on the dark web and know how to report suspicious sites or content to the proper authorities.

❖ Assist peers and family members by teaching at least one simple security habit they learned (e.g., password best practices or two-step verification).

Cybersecurity Vocational Course

Students enrolled in this program will receive:

- **Comprehensive Slide Decks**
  All presentation slides uploaded to the LMS, complete with clear visuals and succinct summaries.

- **Expert Sessions**
  Renowned cybersecurity professionals will present on the latest trends in cybersecurity and cybercrime.

- **Curated Reading References**
  Annotated list of textbooks, articles, blogs, and online resources linked directly from each module's slides.

Students enrolled in this program will receive:

- **Hands-On Lab in Recorded form**
  Step-by-step video demonstrations showing how to install and use key security tools in realistic scenarios.

- **Lecture Recordings**
  Full-length video of every class session, accessible on the LMS.

- **Post-Module Assessments**
  Short quizzes at the end of each module to reinforce learning and track your progress.

Cybersecurity Vocational Course

Module Names		
	Cyber Crime and Cyber Hygiene (5:30 Hours)	• Understanding cyber crime: What it is & how it affects individuals • Categories of cyber crime: Financial fraud, identity theft, cyberstalking, etc. • Laws governing cyber crime in India (IT Act 2000, IPC sections) • Global perspectives on cyber crime (FBI, Interpol reports) • Case Study: Jamtara Scam (India) –Phishing & OTP Fraud • Case Study: Morrisons Insider Data Breach (UK) –Employee Data Theft • Case Study: Morrisons Insider Data Breach (UK) – Employee Data Theft
		Lab Simulation: • Identify phishing messages in real-time examples • Learn how fraudsters operate through social engineering
	Social Media Threats & Cyberbullying (5:30 Hours)	• Fake profiles & impersonation scams • WhatsApp & Telegram frauds (Deepfake videos, sextortion) • Cyberbullying, online harassment & legal protections in India • Safe use of Instagram, Facebook, LinkedIn, and Twitter • Password Security – Video • Case Study: Bulli Bai & Sulli Deals (India) – Misuse of Social Media for Harassment • Case Study: Ashley Madison Hack (Global) – Privacy Breach & Blackmailing • Case Study: Deepfake videos
		Lab Simulation: • How to secure your social media profiles • Recognizing deepfake videos & manipulated images

Cybersecurity Vocational Course

Module Names		
	Identity Theft & Personal Data Leaks (5:30 Hours)	• Aadhaar/PAN card fraud & identity cloning • Mobile SIM fraud & call spoofing • Data leaks from popular websites & apps • Case Study: Aadhaar Data Leak (India) –Government Database Exposure • Case Study: Facebook-Cambridge Analytica (Global) –Privacy Manipulation in Elections
		Lab Simulation: • How to secure your social media profiles • Recognizing deepfake videos & manipulated images
	Online Financial Frauds & Digital Payments Security (5:30 Hours)	• UPI & credit/debit card frauds (skimming, SIM swapping) • Fake investment & job scams • Digital wallet & cryptocurrency frauds • Legal rights of victims in India (How to report cyber frauds) • Case Study: MobiKwik Data Breach (India) – 10 Crore User Records Leaked • Case Study: Nigerian Prince Scam (Global) – Fake Inheritance & Lottery Frauds
		Lab Simulation: • How to verify fake bank emails & websites • Safe digital transactions: Checking website authenticity before making payments

Cybersecurity Vocational Course

Module Names		
	Women & Child Online Safety (5:30 Hours)	• Introduction to Online Safety • Recognizing and Responding to Cyberbullying • Protecting Personal Information and Privacy • Building a Safe Online Community • Case Study: Blue Whale & Momo Challenge (Global) –Dangerous Online Games • Case Study: Airbnb Hidden Camera Scam (Global) –Invasion of Privacy
		Lab Simulation: • How to detect hidden cameras in hotel rooms • Steps to take if you face online harassment
	Awareness on Ransomware (3:00 Hours)	• Introduction to Ransomware • How Ransomware Works • Case Study: WannaCry Ransomware (2017 Global Attack) (15 mins) • Case Study: AIIMS New Delhi (2023) (15 mins) • Preventive Measures & Defensive Awareness

Cybersecurity Vocational Course

Module Names		
	Dark Web, Cyber Terrorism & Illegal Activities (5:30 Hours)	• What is the dark web? Myths vs. reality • Illegal drug markets, human trafficking & hacking services • Cyber terrorism & extremist activities online • Case Study: Case Study: Silk Road Marketplace (Global) –Illegal Drug Trade via Bitcoin • Case Study: Indian Hacking Cartel –Hiring Hackers for Illegal Activities
		Lab Simulation: • How cyber criminals operate on the dark web (Safely using open-source tools) • Recognizing and reporting extremist content online
	Best Practices for Cyber Hygiene (5:30 Hours)	• Recognizing cyber threats before they happen • Safe browsing habits & website security checks • DR and backup • 2F and MFA • Protecting your devices (Phones, laptops, smart TVs)What to do if you become a victim of cyber crime • Case Study: Google & Apple Scams – Fake Apps & Malware Infections
		Lab Simulation: • Identifying safe vs. malicious apps on Google Play Store • Setting up security tools (Antivirus, VPN, Privacy Browsers)

Cybersecurity Vocational Course

❖ Credit Distribution & Weightage

- ❖ **Theory:** 15 hours (1 credit), 40% of total marks
- ❖ **Practical:** 60% of total marks
- ❖ **Lecture Structure**
  - ❖ Total of 45 hours of recorded lectures in Hindi (with English PPTs)
- ❖ **Labs**
  - ❖ Recorded labs provisioned for every module
- ❖ **Student Support**
  - ❖ Regular doubt-clearing sessions after each module
  - ❖ Post-module quizzes to reinforce learning and track progress

Thank You
&
FAQ