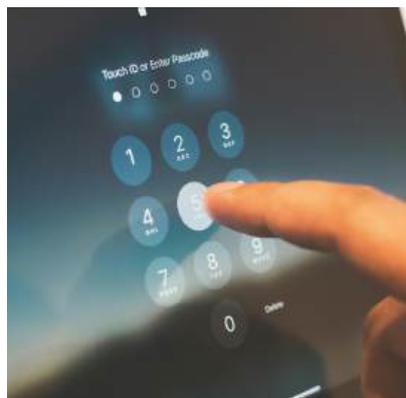


# CYBERSECURITY CURRICULUM: FROM FOUNDATIONS TO ADVANCED PRACTICES

---

This comprehensive Cybersecurity Curriculum is meticulously designed to equip learners with a robust understanding of cybersecurity principles, evolving from fundamental concepts to advanced practical applications. It integrates theoretical knowledge with hands-on skills, preparing individuals to address the complex challenges of the digital security landscape. This program aims to foster critical thinking and practical proficiency essential for safeguarding digital assets and responding to modern cyber threats effectively.

Perfect Connect



# 01 Introduction to Cybersecurity

**Topics Covered:** - Importance of cybersecurity in the digital age - Common cyber threats and attack vectors - Overview of cybersecurity domains

**Learning Outcomes:** - Understand the significance of cybersecurity - Identify various types of cyber threats - Recognize the foundational domains within cybersecurity

**Resources:** - Cisco Networking Academy: Introduction to Cybersecurity - W3Schools Cybersecurity Syllabus

# 02 Networking Fundamentals

**Topics Covered:** - OSI and TCP/IP models - IP addressing and subnetting - Network devices and protocols

**Learning Outcomes:** - Grasp the structure and function of computer networks - Configure basic network settings - Analyze network traffic and identify anomalies

**Resources:** - CompTIA Network+ Certification Guide

# 03 System and Network Security

**Topics Covered:** - Firewalls and intrusion detection/prevention systems (IDS/IPS) - Virtual Private Networks (VPNs) - Secure network design principles

**Learning Outcomes:** - Implement network security measures - Configure and manage firewalls and IDS/IPS - Design secure network architectures

**Resources:** - SANS Cybersecurity Skills Roadmap

# 04 Cryptography

**Topics Covered:** - Symmetric and asymmetric encryption - Hash functions and digital signatures - Public Key Infrastructure (PKI) 1

**Learning Outcomes:** - Understand cryptographic principles - Apply encryption techniques to secure data - Manage digital certificates and keys

**Resources:** - Boston University: Cybersecurity Course Syllabus

# 05 Ethical Hacking and Penetration Testing

**Topics Covered:** - Phases of ethical hacking - Vulnerability assessment tools - Exploitation techniques

**Learning Outcomes:** - Conduct penetration tests ethically - Utilize tools like Metasploit and Nmap Report and remediate vulnerabilities

**Resources:** - Hack The Box: Certified Defensive Security Analyst

# 06 Digital Forensics and Incident Response

**Topics Covered:** - Forensic investigation processes - Evidence collection and preservation - Incident response planning

**Learning Outcomes:** - Perform digital forensic investigations - Develop and implement incident response strategies - Analyze and report on security incidents

**Resources:** - ITU Academy: Cybersecurity Techniques Training Outline

## 07 Cybersecurity Laws and Ethics

**Topics Covered:** - Indian IT Act and global cybersecurity laws - Ethical considerations in cybersecurity Compliance standards (GDPR, HIPAA)

**Learning Outcomes:** - Navigate legal frameworks governing cybersecurity - Uphold ethical standards in security practices - Ensure organizational compliance with relevant laws

**Resources:** - CoSN: Cybersecurity in K12 Education Syllabus

## 08 Advanced Topics and Emerging Trends

**Topics Covered:** - Artificial Intelligence in cybersecurity - Cloud security challenges - Internet of Things (IoT) security

**Learning Outcomes:** - Analyze the impact of emerging technologies on cybersecurity - Implement security measures for cloud and IoT environments - Stay updated with evolving cybersecurity threats and solutions

**Resources:** - AI-assisted Malware Analysis Course

## 09 Cloud Security

**Topics Covered:** - Cloud Identity and Access Management (IAM) - Cloud data protection strategies (encryption, tokenization, key management) - Cloud monitoring and compliance (CSPM, CNAPP, continuous assurance)

**Learning Outcomes:** - Implement robust IAM controls in cloud environments - Protect sensitive data across cloud service models (IaaS, PaaS, SaaS) - Monitor cloud infrastructure for compliance and anomalies

**Resources:** - AWS Security Essentials - Google Cloud Security Foundations - Microsoft Cloud Security Benchmark

## 10 Security Operations and Threat Intelligence

**Topics Covered:** - Security Operations Center (SOC) fundamentals - Threat Intelligence Lifecycle (collection, analysis, dissemination) - Threat hunting and advanced detection techniques

**Learning Outcomes:** - Understand the structure and functions of a SOC - Utilize threat intelligence to predict and prevent cyber threats - Conduct proactive threat hunting using SIEM and EDR tools

**Resources:** - MITRE ATT&CK Framework - SANS Threat Hunting and Incident Response Course

## 11 Product and Application Security

**Topics Covered:** - Secure Software Development Lifecycle (SDLC) - DevSecOps and CI/CD pipeline security - API security fundamentals and best practices

**Learning Outcomes:** - Integrate security across the software development lifecycle - Implement automated security testing in CI/CD environments - Design and protect secure APIs against modern attacks

**Resources:** - OWASP Top 10 - Google DevSecOps Foundations - API Security Alliance Learning Path

