Cyber Security Course

A **Cyber Security course** teaches how to **protect computers, networks, applications, and data** from cyber attacks such as hacking, malware, phishing, and data breaches.

Objectives of a Cyber Security Course

- Understand **cyber threats & attacks**
- Learn **defensive and preventive techniques**
- Secure **networks, systems, and applications**
- Build skills for **ethical hacking & security analysis**
- Prepare for **industry roles & certifications**

Who Can Learn Cyber Security?

✓ School & college students
✓ Beginners in IT
✓ Programmers & network engineers
✓ Career switchers

No hacking background required to start

Career Opportunities

- Cyber Security Analyst
- Ethical Hacker
- SOC Analyst
- Network Security Engineer
- Cloud Security Engineer

Cyber Security Course Syllabus

Module 1: Introduction to Cyber Security (6 Hours)

Objectives

- Understand cyber security fundamentals
- Recognize cyber threats and risks

Topics

- What is Cyber Security?
- Need for Cyber Security
- CIA Triad (Confidentiality, Integrity, Availability)
- Types of cyber attacks
- Cyber crime overview
- Cyber ethics & responsibilities

Outcome: Students understand why cyber security is critical

Module 2: Networking & Internet Fundamentals (10 Hours)

Topics

- Computer networks overview
- TCP/IP vs OSI model
- Internet addressing (IP, MAC, Ports)
- Internet protocols (HTTP, HTTPS, FTP, SMTP, DNS)
- LAN, WAN, MAN
- Routers, switches, firewalls

Practical

- IP configuration
- Ping, traceroute
- Packet flow demonstration

Outcome: Strong networking foundation for security concepts

Module 3: Operating System Security (8 Hours)

Topics

- Windows security basics
- Linux introduction
- User accounts & permissions
- File system security
- Authentication & authorization
- System vulnerabilities

Practical

- Linux basic commands
- File permissions
- User management

Outcome: Students understand OS-level security

Module 4: Cryptography & Data Security (8 Hours)

Topics

- Cryptography fundamentals
- Symmetric encryption (AES)
- Asymmetric encryption (RSA)
- Hashing (MD5, SHA)
- Digital signatures
- SSL/TLS basics

Practical

- Hash generation
- Encryption & decryption demo

Outcome: Clear understanding of secure communication

Module 5: Ethical Hacking Fundamentals (10 Hours)

Topics

- Types of hackers
- Ethical hacking methodology
- Footprinting & reconnaissance
- Scanning & enumeration
- Vulnerability assessment
- Social engineering awareness

⚠ Legal & ethical boundaries emphasized

Practical

- Nmap scanning
- Basic reconnaissance

Outcome: Students learn attacker mindset (ethically)

Module 6: Web Application Security (10 Hours)

Topics

- Web application architecture
- OWASP Top 10
- SQL Injection
- XSS (Cross Site Scripting)
- CSRF
- Secure coding principles

Practical

- Vulnerability testing demo
- Input validation examples

Outcome: Ability to identify common web vulnerabilities

Module 7: Network Security (8 Hours)

Topics

- Firewalls (types & working)
- IDS / IPS
- VPN
- Wireless security
- Network attacks & defense

Practical

- Firewall rule demo
- Packet capture basics

Outcome: Network protection understanding

Module 8: Malware & Threat Management (6 Hours)

Topics

- Types of malware
- Ransomware
- Malware lifecycle
- Antivirus & detection techniques
- Incident response basics

Outcome: Awareness of modern threats

Module 9: Cloud & Emerging Security (6 Hours)

Topics

- Cloud computing basics
- Cloud security challenges
- IAM concepts
- IoT security overview
- AI & Cyber Security (intro)

Outcome: Exposure to modern security domains

Module 10: Cyber Security Tools & Case Studies (8 Hours)

Tools

- Kali Linux overview
- Wireshark
- Nmap
- Burp Suite (intro)

Case Studies

- Data breaches

- Ransomware attacks
- Phishing campaigns

Outcome: Real-world understanding

Assessment & Evaluation

- Quizzes (Module-wise)
- Practical assignments
- Mini project / case study
- Final exam

Course Outcomes

By the end of the course, students will be able to:

- Understand cyber threats and defenses
- Apply basic security practices
- Identify vulnerabilities
- Use essential cyber security tools
- Follow ethical & legal guidelines