# Cyber Security

## Programme Objective:

This programme aims to help the learners to navigate the foundations and skills necessary to build a career in the field of cyber security.

## Expected Outcome:

After completion of this programme the learners will be able to understand the basic security objectives and the countermeasure the threats by using various security models and mechanisms.

# Syllabus

| Theory | | |
|---|---|---|
| **Module** | **Chapter No.** | **Topic** |
| **Module – 1** Introduction to Information Security and Potential Threats | Chapter – 1 | Introduction to Cyber Space, Cyber Security and Information Systems |
| | Chapter – 2 | Cyber Attacks and their Classification |
| | Chapter – 3 | Types of Malware and Threats |
| **Module – 2** Cyber Vulnerability and Network Security | Chapter – 4 | Assessment of Vulnerability |
| | Chapter – 5 | Intrusion : Detection and Prevention Systems |
| | Chapter – 6 | Internet Protocols, Operating System Security and Network Security |
| **Module – 3** User Authentication Tools and Information Security Models | Chapter – 7 | User Authentication Methods, |
| | Chapter – 8 | Information Security Models and Security Mechanisms |
| | Chapter – 9 | Biometric Systems and Biometric Authentication Processes |
| **Module – 4** Web and Mobile App security Methods | Chapter – 10 | Web Security and Email Security |
| | Chapter – 11 | Security of Mobile Devices and Cloud Space |
| | Chapter – 12 | Social Media Security and IoT Security |
| **Module – 5** Cyber Crimes and Digital Forensic Science | Chapter – 13 | Cyber Crimes, Scams and Frauds |
| | Chapter – 14 | Digital Forensic Investigation Methods, Cyber Trails |
| | Chapter – 15 | Branches of Digital Forensics, Reporting, Management of Evidence |
| **Module – 6** Prohibitory Laws for Cyber Security | Chapter – 16 | Jurisdiction of Cyber Crime, Information Technology Act 2000 and its Amendments |
| | Chapter – 17 | Validity of Digital Communication Evidences (Call Records /Emails/SMS) |
| | Chapter – 18 | RBI Act and IPR Act |

| Practical | | |
|---|---|---|
| **Module – 7**<br>Practical | Practical – 1 | Performing the web security audit and report preparation |
| | Practical – 2 | Biometric Authentication Processes |
| | Practical – 3 | Explore the Nmap tool and list how it can be used for network defense. |
| | Practical – 4 | Explore the NetCat tool |
| | Practical – 5 | Examine SQL injection attack |
| | Practical – 6 | Perform online attacks and offline attacks of password cracking. |
| | Practical – 7 | Evaluate network defense tools for DOS attack |
| | Practical – 8 | Evaluate network defense tools for IP spoofing |
| | Practical – 9 | Consider a case study of cyber crime, where the attacker has performed online debit card fraud. Prepare a report and also list the laws to be imposed on attacker |
| | Practical – 10 | To ensure Security of any one web browser (Mozilla Firefox/Google Chrome) |
| | Practical – 11 | Set Firewall security for windows |
| | Practical – 12 | To gather information from any PC's connected to the LAN |

## Course Duration :

Theory : 18 Hours
Practical : 12 Hours