

UNIT I: CYBER SPACE AND DIGITAL SECURITY

Module 1: Introduction to Cyber Space

What is Cyber Space?

Cyber Space is a virtual environment where people communicate, share information, and perform activities using computers, mobile devices, and the Internet.

It includes:

- Internet
- Computers
- Mobile phones
- Networks
- Websites
- Cloud services
- Social media

Cyber space is not a physical place. It is a digital world where information is stored, processed, and transmitted.

Features of Cyber Space

- Global connectivity
- Fast communication
- Information sharing
- Online services
- Digital transactions
- 24×7 availability

Uses of Cyber Space

- Education
- Online banking
- E-commerce
- Social networking
- Entertainment
- Healthcare

- Government services

Advantages

- Easy communication
- Quick access to information
- Online learning
- Digital payments
- Business growth

Disadvantages

- Cyber crimes
- Privacy issues
- Fake news
- Identity theft
- Data breaches

Module 2: Evolution of the Internet and Digital Society

Evolution of the Internet

The Internet started as a small research network and has now become a worldwide communication system.

Major Stages

1969 – ARPANET

- First computer network developed by the U.S. Department of Defense.

1983 – TCP/IP

- Standard communication protocol adopted.

1990 – World Wide Web (WWW)

- Invented by Tim Berners-Lee.
- Made the Internet easy to use.

2000 onwards

- Broadband Internet

- Smartphones
- Social media
- Cloud computing
- Artificial Intelligence

Digital Society

A Digital Society is a society where most activities are performed using digital technologies.

Examples:

- Online education
- Digital banking
- Digital payments
- Online shopping
- Telemedicine
- E-governance

Benefits

- Better communication
- Faster services
- Increased productivity
- Easy access to information

Challenges

- Cyber attacks
- Privacy concerns
- Digital divide
- Fake information

Module 3: Digital Ecosystems and Online Platforms

Digital Ecosystem

A Digital Ecosystem is a group of connected digital technologies, users, organizations, and services that work together.

Components

- Users
- Devices
- Networks
- Software
- Cloud services
- Data

Examples

- Google ecosystem
- Microsoft ecosystem
- Apple ecosystem

Online Platforms

Online platforms allow users to communicate, learn, shop, or work over the Internet.

Examples:

- Social media
- E-commerce websites
- Online banking
- Video conferencing
- Learning Management Systems (LMS)

Advantages

- Easy access
- Time saving
- Better communication
- Online collaboration

Risks

- Fake accounts
- Online fraud
- Privacy leakage
- Malware attacks

Module 4: Concept of Cyber Security

What is Cyber Security?

Cyber Security is the practice of protecting computers, networks, software, and data from cyber attacks.

Objectives

- Protect data
- Protect systems
- Ensure safe online activities
- Prevent unauthorized access

Need for Cyber Security

- Increase in online transactions
- Growth of cyber crimes
- Protection of personal information
- Secure government and business data

Types of Cyber Security

- Network Security
- Application Security
- Information Security
- Cloud Security
- Mobile Security
- Endpoint Security

Benefits

- Protects confidential data

- Reduces cyber risks
- Improves trust
- Ensures business continuity

Module 5: Confidentiality, Integrity, and Availability (CIA Triad)

The CIA Triad is the foundation of Information Security.

1. Confidentiality

Confidentiality means information should only be accessible to authorized users.

Methods

- Passwords
- Encryption
- Authentication
- Access control

Example:

Only a bank customer can view their account details.

2. Integrity

Integrity means data should remain accurate and unchanged.

Methods

- Hashing
- Digital signatures
- Backups
- Checksums

Example:

Exam results should not be modified by unauthorized persons.

3. Availability

Availability means information and services should be accessible whenever required.

Methods

- Regular backups
- UPS
- Disaster recovery
- Redundant servers

Example:

Online banking should be available throughout the day.

Module 6: Digital Identity and Personal Data

Digital Identity

Digital Identity is the online identity of a person.

It includes:

- Username
- Password
- Email address
- Mobile number
- Aadhaar number
- Digital certificates

Importance

- Secure login
- Online authentication
- Access to digital services

Personal Data

Personal Data is any information that identifies an individual.

Examples:

- Name
- Address
- Mobile number

- Email
- Aadhaar number
- PAN number
- Bank account details
- Biometric information

Sensitive Personal Data

- Fingerprints
- Face recognition
- Health records
- Financial information
- Passwords

Protection Methods

- Strong passwords
- Two-factor authentication
- Encryption
- Avoid sharing personal information
- Update software regularly

Module 7: Privacy and Data Protection Issues

Privacy

Privacy means protecting personal information from unauthorized access.

Privacy Issues

- Data collection without consent
- Tracking online activities
- Identity theft
- Social media misuse
- Unauthorized sharing of information

Data Protection

Data Protection means safeguarding personal information from misuse, loss, or theft.

Importance

- Protects personal information
- Prevents financial fraud
- Maintains trust
- Ensures legal compliance

Good Practices

- Use strong passwords
- Enable two-factor authentication
- Update software regularly
- Avoid suspicious links
- Backup important files
- Review privacy settings

Module 8: Cyber Risks in Daily Digital Life

Cyber Risks

Cyber Risks are dangers that may cause loss of data, money, or privacy while using digital technologies.

Common Cyber Risks

- Phishing emails
- Fake websites
- Malware
- Ransomware
- Identity theft
- Online banking fraud
- Social media scams
- Data leakage

Safe Online Practices

- Use strong and unique passwords.
- Enable two-factor authentication.
- Do not share OTPs or passwords.
- Verify website URLs before entering personal information.
- Install antivirus software.
- Update operating systems and applications regularly.
- Avoid downloading files from unknown sources.
- Be careful while using public Wi-Fi.
- Backup important data regularly.

Online Frauds and Cyber Crimes

Module 1: Understanding Cyber Crimes

Introduction

A cyber crime is any illegal activity carried out using computers, mobile phones, the Internet, or digital devices. Cyber criminals use technology to steal money, personal information, or damage computer systems.

As Internet usage and digital payments increase, cyber crimes are becoming more common.

Characteristics of Cyber Crimes

- Committed using computers or mobile devices.
- Can occur from anywhere in the world.
- Often target individuals, businesses, and government organizations.
- May cause financial loss and identity theft.
- Difficult to trace if proper security measures are not followed.

Common Examples

- Hacking
- Phishing

- Identity theft
- Online banking fraud
- Cyber bullying
- Ransomware attacks
- Social media fraud
- Online shopping scams

Effects of Cyber Crimes

- Financial loss
- Loss of personal data
- Damage to reputation
- Privacy violations
- Emotional stress

Prevention

- Use strong passwords.
- Enable Two-Factor Authentication (2FA).
- Avoid suspicious links.
- Keep software updated.
- Report cyber crimes immediately.

Module 2: Classification of Online Frauds

What is an Online Fraud?

An online fraud is a dishonest act carried out through the Internet to cheat people and steal money or personal information.

Types of Online Frauds

Phishing Fraud

Fake emails or websites steal login details.

Vishing Fraud

Fraud through phone calls.

Smishing Fraud

Fraud through SMS or messaging apps.

Banking Fraud

Illegal access to bank accounts.

UPI Fraud

Unauthorized digital payment transactions.

Card Fraud

Misuse of debit or credit card information.

Identity Theft

Using another person's personal information.

Social Media Fraud

Fake accounts and fraudulent messages.

E-commerce Fraud

Fake online shopping websites.

Investment Scam

Promises of very high returns to attract victims.

Job Scam

Fake job offers asking for registration or processing fees.

Module 3: Phishing and Email-Based Frauds

What is Phishing?

Phishing is a cyber attack in which criminals send fake emails or create fake websites to steal sensitive information.

Common Targets

- Bank accounts
- Email accounts
- Social media accounts
- Online shopping accounts

Signs of Phishing Emails

- Unknown sender
- Urgent messages
- Spelling mistakes
- Fake website links
- Requests for passwords or OTP

Prevention

- Verify sender addresses.
- Never share passwords or OTP.
- Do not click unknown links.
- Use spam filters.
- Report suspicious emails.

Module 4: Vishing and Telecommunication Scams

What is Vishing?

Vishing (Voice Phishing) is a fraud where criminals use phone calls to obtain confidential information.

Common Vishing Scams

- Fake bank officials
- Fake police officers
- Lottery prize calls

- KYC verification calls
- Customer care fraud

Prevention

- Never share OTP or PIN.
- Verify the caller's identity.
- Disconnect suspicious calls.
- Contact the organization directly using official numbers.

Module 5: Smishing and Mobile-Based Frauds

What is Smishing?

Smishing (SMS Phishing) is a fraud carried out through SMS or messaging applications.

Common Examples

- Fake parcel delivery messages.
- Fake bank alerts.
- Fake KYC update messages.
- Fake reward or lottery messages.

Warning Signs

- Unknown links
- Urgent requests
- Offers that seem too good to be true
- Requests for personal information

Prevention

- Do not click unknown links.
- Delete suspicious messages.

- Verify information with official sources.
- Install security updates regularly.

Module 6: Online Banking and UPI Frauds

Online Banking Fraud

Online banking fraud involves unauthorized access to bank accounts to steal money.

Common Banking Frauds

- Phishing
- Fake banking apps
- OTP fraud
- SIM swap fraud
- Remote access app fraud

UPI Fraud

UPI (Unified Payments Interface) enables instant money transfers.

Fraudsters misuse UPI by:

- Sending fake payment requests.
- Sharing fake QR codes.
- Pretending to be buyers or sellers.
- Creating fake customer care services.

Safe Banking Practices

- Never approve unknown payment requests.
- Verify UPI IDs carefully.
- Never share OTP or PIN.
- Use official banking applications.
- Enable transaction alerts.

Module 7: Card and Payment Gateway Frauds

Card Fraud

Card fraud occurs when someone illegally uses another person's debit or credit card information.

Common Types

ATM Skimming

Hidden devices copy card details.

Card Cloning

Duplicate cards are created.

Online Card Fraud

Card details are stolen during online shopping.

Fake Payment Gateway

Fraudulent websites collect payment information.

Prevention

- Cover keypad while entering PIN.
- Use secure websites (HTTPS).
- Monitor bank statements.
- Report lost cards immediately.
- Enable SMS alerts.

Module 8: Identity Theft and Impersonation

Identity Theft

Identity theft is the unauthorized use of another person's personal information.

Personal Information That May Be Stolen

- Aadhaar number
- PAN number
- Bank account details
- Mobile number
- Email account
- Passwords

Impersonation

Impersonation means pretending to be another person online for fraudulent purposes.

Examples:

- Fake social media profiles
- Fake customer care executives
- Fake government officials

Prevention

- Protect personal information.
- Enable Two-Factor Authentication.
- Use strong passwords.
- Monitor financial accounts regularly.

Module 9: Social Media Frauds

Introduction

Social media platforms are commonly targeted by cyber criminals.

Common Frauds

- Fake profiles
- Fake giveaways
- Romance scams

- Account hacking
 - Fake charity requests
 - Fake investment groups
-

Prevention

- Accept requests only from known people.
- Check privacy settings.
- Do not share sensitive information.
- Report fake accounts.
- Enable Two-Factor Authentication.

Module 10: E-commerce and Marketplace Scams

What is E-commerce?

E-commerce refers to buying and selling goods and services online.

Common Scams

- Fake shopping websites
- Fake sellers
- Non-delivery of products
- Counterfeit products
- Fake refund messages
- Payment before delivery fraud

Safe Online Shopping

- Buy from trusted websites.
- Read customer reviews.
- Verify seller information.
- Use secure payment methods.

- Avoid unbelievable discounts.

Module 11: Investment and Job Frauds

Investment Fraud

Fraudsters promise high returns with little or no risk.

Examples:

- Cryptocurrency scams
- Ponzi schemes
- Fake trading platforms
- Fake stock market tips

Job Fraud

Fake recruiters offer jobs after collecting registration fees.

Warning Signs

- Guaranteed high income.
- Advance payment requests.
- Fake appointment letters.
- Interviews through unofficial platforms only.

Prevention

- Verify companies.
- Never pay for job offers.
- Research investment opportunities.
- Read official reviews.

Module 12: Social Engineering Techniques

What is Social Engineering?

Social engineering is the psychological manipulation of people to obtain confidential information or gain unauthorized access.

Instead of attacking computers, cyber criminals target human behavior.

Common Social Engineering Techniques

Phishing

Fake emails requesting confidential information.

Vishing

Phone call scams.

Smishing

SMS-based frauds.

Pretexting

Creating a false story to gain trust.

Baiting

Offering free gifts or downloads to trick users.

Tailgating

Unauthorized person enters a secure area by following an authorized person.

Prevention

- Verify identities before sharing information.
- Never disclose passwords or OTPs.
- Be cautious with unexpected requests.
- Think before clicking links.
- Report suspicious activities immediately.

Key Terms

Term	Meaning
Cyber Crime	Illegal activity using computers or the Internet

Term	Meaning
Online Fraud	Cheating through digital platforms
Phishing	Fake emails or websites used to steal information
Vishing	Fraud through phone calls
Smishing	Fraud through SMS or messaging apps
UPI Fraud	Fraud involving Unified Payments Interface transactions
Card Fraud	Unauthorized use of debit or credit card details
Identity Theft	Stealing and misusing another person's personal information
Impersonation	Pretending to be someone else for fraud
Social Engineering	Manipulating people to reveal confidential information

Unit III: Cyber Security Practices and Tools

Module 1: Password Security and Authentication

Introduction

A password is a secret combination of letters, numbers, and symbols used to protect digital accounts and devices. Strong passwords help prevent unauthorized access and protect personal information.

Authentication is the process of verifying the identity of a user before granting access to a computer system or online service.

Importance of Strong Passwords

- Protects personal and financial information.
- Prevents unauthorized access.
- Secures online accounts.
- Reduces the risk of cyber attacks.
- Protects confidential data.

Characteristics of a Strong Password

A strong password should:

- Be at least 12 characters long.
- Include uppercase and lowercase letters.
- Contain numbers.
- Include special characters such as @, #, \$, %.
- Be unique for each account.
- Avoid personal information like names or birthdays.

Example of a Strong Password:

- R@vi2026#Secure

Weak Password Examples

- 123456
- password
- abc123
- india123
- qwerty

These passwords are easy to guess and should never be used.

Password Management

Password management means creating, storing, and updating passwords securely.

Good Practices

- Use different passwords for different accounts.
- Change passwords regularly.
- Never share passwords.
- Store passwords safely.
- Avoid writing passwords where others can see them.

Authentication

Authentication confirms that a user is genuine.

Types of Authentication

1. Password-Based Authentication

Uses a username and password.

2. Two-Factor Authentication (2FA)

Requires two verification methods.

Example:

- Password + OTP

3. Multi-Factor Authentication (MFA)

Uses two or more methods such as:

- Password
- OTP
- Fingerprint
- Face recognition

Benefits of Multi-Factor Authentication

- Provides extra security.
- Reduces hacking risks.
- Protects banking accounts.
- Prevents identity theft.

Module 2: Malware, Ransomware, and Spyware

What is Malware?

Malware (Malicious Software) is software designed to damage computers, steal information, or disrupt normal operations.

Types of Malware

Virus

- Attaches itself to files.
- Spreads when infected files are shared.

Worm

- Spreads automatically through networks.
- Does not require user action.

Trojan Horse

- Appears to be useful software.
- Performs malicious activities secretly.

Spyware

Spyware secretly collects user information such as:

- Passwords
- Browsing history
- Banking information

Ransomware

Ransomware encrypts files and demands money (ransom) to restore access.

Effects of Malware

- Data loss
- Slow computer performance
- Financial loss
- Identity theft
- Privacy violations

Prevention

- Install antivirus software.
- Avoid unknown email attachments.
- Download software only from trusted websites.
- Update operating systems regularly.

- Scan USB drives before use.

Module 3: Antivirus and Firewall Basics

Antivirus

Antivirus is software that detects, blocks, and removes malware from computers and mobile devices.

Functions of Antivirus

- Detects viruses.
- Removes malware.
- Protects files.
- Scans USB devices.
- Provides real-time protection.

Importance of Antivirus

- Protects personal data.
- Prevents malware infections.
- Improves system security.
- Detects suspicious files.

Firewall

A firewall is a security system that monitors and controls incoming and outgoing network traffic.

It acts as a barrier between a trusted network and the Internet.

Types of Firewalls

Hardware Firewall

Installed between a network and the Internet.

Software Firewall

Installed on individual computers.

Benefits of Firewall

- Blocks unauthorized access.
- Prevents hacking attempts.
- Protects network resources.
- Filters harmful traffic.

Difference between Antivirus and Firewall

Antivirus	Firewall
Detects and removes malware	Controls network traffic
Protects files and programs	Protects networks
Works inside the computer	Works between networks
Removes viruses	Blocks unauthorized connections

Module 4: Email and Cloud Security

Email Security

Email security protects email accounts from cyber attacks.

Common Email Threats

Phishing

Fake emails steal passwords and banking details.

Spam

Unwanted emails that may contain advertisements or malicious links.

Email Spoofing

Attackers send emails using fake sender addresses.

Malicious Attachments

Attachments may contain malware.

Safe Email Practices

- Verify sender addresses.
 - Avoid clicking suspicious links.
 - Scan attachments.
 - Never share passwords through email.
 - Use spam filters.
-

Cloud Computing

Cloud computing allows users to store and access data over the Internet instead of local storage.

Examples:

- Google Drive
- OneDrive
- Dropbox

Cloud Security

Cloud security protects data stored online.

Good Practices

- Use strong passwords.
- Enable Two-Factor Authentication.
- Share files only with trusted users.
- Backup important files.
- Review file sharing permissions regularly.

Module 5: Mobile Device and Network Security

Mobile Security

Smartphones store personal, financial, and professional information, making them important targets for cyber criminals.

Mobile Security Risks

- Malicious apps
- Data theft
- Fake Wi-Fi networks
- Mobile malware
- Lost or stolen devices

Mobile Security Measures

- Use screen lock.
- Install apps only from official app stores.
- Keep software updated.
- Enable device encryption.
- Backup important data.
- Turn off Bluetooth when not in use.

Network Security

Network security protects computers and devices connected through wired or wireless networks.

Safe Wi-Fi Practices

- Use password-protected Wi-Fi.
- Avoid public Wi-Fi for banking.
- Change default router passwords.
- Keep router firmware updated.
- Disable unused wireless features.

Payment Security

Digital payments include:

- UPI
- Debit Cards
- Credit Cards
- Mobile Wallets
- Internet Banking

Safety Tips

- Never share OTP.
 - Verify payment requests.
 - Use official payment apps.
 - Check transaction alerts.
 - Log out after transactions.
-

Module 6: Cyber Hygiene and Safe Digital Practices

What is Cyber Hygiene?

Cyber hygiene refers to the regular practices followed to maintain the security of digital devices, accounts, and online information.

Just as personal hygiene keeps us healthy, cyber hygiene keeps our digital life secure.

Importance of Cyber Hygiene

- Prevents cyber attacks.
- Protects personal information.
- Improves device security.
- Reduces identity theft.
- Ensures safe Internet use.

Good Cyber Hygiene Practices

Password Safety

- Create strong passwords.
- Change passwords periodically.
- Use different passwords for different accounts.

Software Updates

- Install operating system updates.
- Update applications regularly.

Safe Browsing

- Visit trusted websites.
- Check HTTPS before entering sensitive information.
- Avoid suspicious links.

Backup Data

Regularly back up important files using:

- External hard drives
- Cloud storage

Safe Social Media

- Limit personal information shared online.
- Review privacy settings.
- Accept friend requests only from known people.

Device Security

- Lock devices when not in use.
- Install antivirus software.
- Enable automatic updates.

Key Terms

Term	Meaning
Password	Secret code used to access an account or device

Term	Meaning
Authentication	Process of verifying a user's identity
Two-Factor Authentication (2FA)	Login using two verification methods
Malware	Malicious software designed to harm systems
Virus	Malware that infects files and spreads
Spyware	Software that secretly collects user information
Ransomware	Malware that encrypts files and demands payment
Antivirus	Software that detects and removes malware
Firewall	Security system that filters network traffic
Phishing	Fake messages or emails used to steal information
Cloud Computing	Storing and accessing data over the Internet
Cyber Hygiene	Safe practices for protecting digital devices and data

Unit IV: Cyber Laws and Institutional Framework in India

Module 1: Introduction to Cyber Laws in India

Introduction

Cyber law refers to the set of laws that govern the use of computers, digital devices, the Internet, and online activities. These laws help prevent cyber crimes, protect users' rights, and ensure safe use of technology.

With the rapid growth of digital services, online banking, e-commerce, and social media, cyber laws have become essential in India.

Objectives of Cyber Laws

- Prevent cyber crimes.
- Protect personal and financial information.
- Promote safe use of the Internet.
- Recognize electronic records and digital signatures.

- Regulate online transactions.
- Ensure privacy and data security.

Need for Cyber Laws

- Increase in online frauds.
- Growth of digital payments.
- Protection of personal information.
- Secure online communication.
- Safe e-commerce and online banking.
- Protection against hacking and cyber attacks.

Advantages of Cyber Laws

- Legal protection for Internet users.
- Secure online business transactions.
- Encourages digital governance.
- Supports digital economy.
- Builds trust in online services.

Module 2: Information Technology Act, 2000

Introduction

The Information Technology (IT) Act, 2000 is India's primary law dealing with cyber crimes, electronic records, and digital transactions.

It came into force on 17 October 2000.

The Act provides legal recognition to electronic records and digital signatures and defines punishments for cyber offences.

Objectives of the IT Act

- Promote e-commerce.
- Recognize electronic documents.
- Recognize digital signatures.
- Prevent cyber crimes.
- Protect electronic data.

- Encourage e-governance.

Important Features

Electronic Records

Electronic documents are legally valid.

Digital Signatures

Digital signatures can be used to authenticate electronic documents.

E-Governance

Government services can be delivered electronically.

Cyber Crime Provisions

The Act defines various cyber offences and punishments.

Data Protection

Organizations are expected to protect sensitive personal information.

Importance of the IT Act

- Supports Digital India.
- Promotes online banking.
- Facilitates electronic contracts.
- Improves e-governance.
- Helps investigate cyber crimes.

Module 3: Cyber Offences and Penalties

What is a Cyber Offence?

A cyber offence is any illegal activity committed using computers, mobile devices, networks, or the Internet.

Common Cyber Offences

Hacking

Unauthorized access to a computer or network.

Identity Theft

Using another person's personal information without permission.

Phishing

Stealing confidential information through fake emails, messages, or websites.

Online Banking Fraud

Illegal transfer of money from bank accounts.

Cyber Stalking

Repeated online harassment or monitoring of a person.

Cyber Bullying

Using digital platforms to threaten, insult, or harass others.

Malware Attack

Spreading harmful software to damage systems or steal data.

Ransomware

Encrypting files and demanding payment to restore access.

Data Theft

Stealing confidential or personal information.

Website Defacement

Changing the appearance or content of a website without permission.

Penalties

Depending on the offence, punishments may include:

- Monetary fines.
- Imprisonment.
- Compensation to victims.
- Confiscation of electronic devices.
- Other legal actions under the IT Act and related laws.

Module 4: Data Protection and Privacy Rights

What is Data?

Data refers to information stored electronically, such as:

- Name

- Address
- Mobile number
- Aadhaar number
- Bank details
- Email address
- Health information

What is Data Protection?

Data protection means safeguarding personal information from unauthorized access, misuse, loss, or theft.

Privacy Rights

Privacy means a person's right to control how their personal information is collected, used, and shared.

Every individual should have control over their personal data.

Importance of Data Protection

- Protects personal identity.
- Prevents identity theft.
- Builds trust in digital services.
- Secures financial information.
- Protects confidential data.

Good Practices

- Use strong passwords.
- Enable Two-Factor Authentication (2FA).
- Share personal information only with trusted organizations.
- Update software regularly.
- Avoid suspicious links.
- Review app permissions before installing applications.

Module 5: Cyber Crime Reporting Mechanisms

Introduction

Cyber crimes should be reported immediately so that authorities can investigate the incident and help prevent further damage.

How to Report Cyber Crime

National Cyber Crime Reporting Portal

Citizens can report cyber crimes online through the Government of India portal.

Cyber Crime Helpline

Victims of financial cyber fraud can contact the national cyber crime helpline for immediate assistance.

Cyber Police Station

Complaints can be filed at the nearest cyber police station.

Local Police Station

Cyber crime complaints can also be registered at any police station.

Bank Reporting

If banking fraud occurs, immediately inform the concerned bank to block transactions.

Information Required While Reporting

- Date and time of the incident.
- Screenshots or evidence.
- Mobile number or email involved.
- Transaction details (if financial fraud).
- Website or application used.
- Copies of messages or emails.

Importance of Timely Reporting

- Helps recover lost money in some cases.
- Prevents further fraud.
- Assists investigation.
- Protects other users.

Module 6: Role of CERT-In and Cyber Police

What is CERT-In?

CERT-In (Indian Computer Emergency Response Team) is the national agency responsible for responding to cyber security incidents in India.

Functions of CERT-In

- Monitors cyber security incidents.
- Issues security alerts and advisories.
- Coordinates responses to cyber attacks.
- Provides technical guidance.
- Promotes cyber security awareness.
- Supports organizations during cyber emergencies.

What is Cyber Police?

Cyber Police are specialized police units trained to investigate cyber crimes.

Functions of Cyber Police

- Register cyber crime complaints.
- Investigate cyber offences.
- Collect digital evidence.
- Arrest cyber criminals.
- Assist victims.
- Coordinate with banks and Internet service providers.

Other Important Organizations

Ministry of Electronics and Information Technology (MeitY)

- Develops policies related to information technology.
- Promotes digital governance and cyber security initiatives.

Indian Cyber Crime Coordination Centre (I4C)

- Coordinates efforts to combat cyber crime.
- Supports law enforcement agencies.
- Conducts cyber crime awareness programmes.

Reserve Bank of India (RBI)

- Issues cyber security guidelines for banks and digital payment systems.

- Promotes safe digital banking practices.

Key Terms

Term	Meaning
Cyber Law	Laws governing online activities and digital systems
IT Act, 2000	Main cyber law of India
Cyber Offence	Crime committed using computers or the Internet
Privacy	Right to protect personal information
Data Protection	Safeguarding personal data from misuse
CERT-In	National agency for cyber incident response
Cyber Police	Specialized police unit for cyber crime investigation
Digital Signature	Electronic method of verifying the authenticity of a document
Phishing	Fraudulent attempt to steal confidential information
Identity Theft	Misuse of another person's personal information

Unit V: Case Studies, Ethics, and Emerging Cyber Risks

Module 1: Case Studies of Cyber Frauds in India

Introduction

Cyber fraud is a crime committed using computers, mobile phones, or the Internet to steal money, personal information, or confidential data. India has witnessed a rapid increase in cyber frauds due to growing digital payments and online services.

Common Types of Cyber Frauds

1. UPI Payment Fraud

- Fraudsters send fake payment requests.
- Victims unknowingly approve transactions.
- QR code scams are also common.

2. OTP Fraud

- Criminals pretend to be bank officials.
- They ask for OTP (One Time Password).
- OTP is used to transfer money illegally.

3. Fake Customer Care Scam

- Fake customer support numbers are posted online.
- Victims call these numbers and are tricked into installing remote access apps.

4. KYC Update Scam

- Victims receive messages asking them to update KYC.
- Clicking fake links leads to theft of banking information.

5. Online Shopping Fraud

- Fake websites sell products at very low prices.
- After payment, products are never delivered.

6. Investment Scam

- Fake investment apps promise high returns.
- People lose money after investing.

Lessons Learned

- Never share OTP, PIN or passwords.

- Verify websites before making payments.
- Avoid unknown links.
- Enable two-factor authentication.

Module 2: Cyber Security Issues in Banking and FinTech

Introduction

Banking has become digital through Internet Banking, Mobile Banking, UPI, Digital Wallets and FinTech applications.

While these services provide convenience, they also increase cyber security risks.

Major Threats

Phishing

Fake emails or SMS steal login credentials.

Malware

Malicious software steals banking information.

ATM Skimming

Devices secretly copy ATM card information.

SIM Swap Fraud

Fraudsters obtain duplicate SIM cards and receive OTPs.

Mobile Banking Malware

Fake banking apps steal user credentials.

Security Measures

- Strong passwords
- Two-Factor Authentication (2FA)
- Secure banking applications
- Regular software updates
- Transaction alerts
- Encryption

Safe Banking Practices

- Never share OTP.
- Use official banking apps.
- Check account statements regularly.
- Log out after banking sessions.

Module 3: Cyber Risks in E-Governance

What is E-Governance?

E-Governance means delivering government services using Information and Communication Technology (ICT).

Examples:

- Online tax payment
- Digital certificates
- Online passport services
- Aadhaar services
- DigiLocker

Cyber Risks

Data Breach

Unauthorized access to government databases.

Identity Theft

Stealing citizens' identity information.

Website Defacement

Hackers change government websites.

DDoS Attack

Government websites become unavailable due to excessive traffic.

Ransomware

Important government data is encrypted by attackers.

Protection Measures

- Secure government networks

- Regular backups
- Employee awareness
- Encryption
- Strong authentication
- Security audits

Module 4: Ethics and Responsible Use of Technology

What is Cyber Ethics?

Cyber ethics refers to moral principles for using computers and the Internet responsibly.

Principles of Cyber Ethics

Respect Privacy

Do not access others' personal information.

Respect Intellectual Property

Do not copy software or books illegally.

Responsible Communication

Avoid abusive language online.

Honesty

Do not spread fake information.

Digital Citizenship

Use technology responsibly.

Unethical Activities

- Cyberbullying
- Software piracy
- Identity theft
- Plagiarism
- Online harassment
- Hacking

Responsible Internet Use

- Verify information before sharing.
- Respect others online.
- Follow cyber laws.
- Report cyber crimes.

Module 5: Artificial Intelligence and Cyber Threats

What is Artificial Intelligence (AI)?

Artificial Intelligence (AI) enables computers to perform tasks that normally require human intelligence.

Examples:

- Chatbots
- Voice assistants
- Recommendation systems
- Face recognition

Positive Uses of AI in Cyber Security

- Detects malware quickly.
- Identifies suspicious activities.
- Prevents phishing attacks.
- Detects network intrusions.
- Automates threat detection.

Cyber Threats Using AI

- AI-generated phishing emails
- Password cracking
- Fake voice generation
- Intelligent malware
- Automated cyber attacks

Prevention

- AI-based security software

- User awareness
- Regular software updates
- Strong authentication

Module 6: Deepfakes and Automated Frauds

What are Deepfakes?

Deepfakes are fake images, videos, or audio created using Artificial Intelligence that appear real.

Uses of Deepfakes

Positive Uses

- Movies
- Education
- Entertainment
- Language translation

Misuse

- Fake news
- Financial fraud
- Political manipulation
- Identity theft
- Reputation damage

Automated Frauds

Cyber criminals use automation for:

- Sending phishing emails
- Fake phone calls
- Social media scams
- Fake customer support

Safety Measures

- Verify videos from trusted sources.

- Cross-check news.
- Do not trust unknown voice messages.
- Report suspicious content.

Module 7: Internet of Things (IoT) and Security Risks

What is IoT?

Internet of Things (IoT) refers to physical devices connected to the Internet.

Examples

- Smart TV
- Smart Watch
- Smart Bulbs
- CCTV Cameras
- Smart Home Devices
- Smart Cars

Security Risks

Weak Passwords

Default passwords can be easily guessed.

Unpatched Devices

Old software contains vulnerabilities.

Data Privacy

IoT devices collect personal information.

Device Hijacking

Hackers take control of devices.

Botnets

Compromised IoT devices are used for cyber attacks.

Security Best Practices

- Change default passwords.
- Update firmware regularly.

- Disable unused features.
- Use secure Wi-Fi.
- Buy trusted IoT devices.

Module 8: Future of Cyber Security in India

Emerging Trends

Artificial Intelligence Security

AI helps detect cyber attacks automatically.

Zero Trust Security

Every user and device must be verified before access.

Cloud Security

Protecting data stored in cloud platforms.

Quantum Computing

Future computers may challenge current encryption methods.

Cyber Security Awareness

Digital literacy and awareness programs are increasing.

Stronger Cyber Laws

Governments continue to strengthen cyber security regulations.

Career Opportunities

- Cyber Security Analyst
- Ethical Hacker
- Digital Forensics Expert
- Security Consultant
- Network Security Engineer
- Incident Response Analyst
- Cloud Security Specialist