Unit-wise Question Bank – Introduction to Cyber Security

UNIT – I: Information Security Fundamentals & Best Practices

Part-A (2 Marks – Short Answer)

1. Define Information Security.

Information Security is the practice of protecting information from unauthorized access, use, disclosure, modification, or destruction.

It ensures three main objectives (CIA Triad):

- **Confidentiality** → Only authorized users can access the information.
- **Integrity** → Information remains accurate and unaltered.
- **Availability** → Information is accessible to authorized users when needed.

Example:
Protecting your online banking account by using a strong password, two-factor authentication, and encryption to prevent hackers from stealing your data.

2. What is meant by "Compromised Computer"?

A Compromised Computer is a computer system that has been breached or taken over by an unauthorized person, often through malware, hacking, or security vulnerabilities.

Once compromised, the attacker can:

- Steal sensitive information
- Install malicious software
- Use the computer to launch attacks on other systems
- Spy on the user's activities

Example:
If your laptop is infected with a Trojan horse, a hacker might control it remotely to send spam emails or mine cryptocurrency without your knowledge.

3. List two safe internet usage practices.

Two **safe internet usage practices** are:

1. **Use strong, unique passwords** for each online account — mix letters, numbers, and symbols to make them hard to guess.
2. **Avoid clicking suspicious links or attachments** in emails, messages, or pop-ups, as they may lead to phishing or malware.

Example:
Using a password like Gm@!2yX#7p instead of password123 and ignoring an email claiming "You've won a prize — click here!"

4. Write the importance of securing computer networks.

Importance of Securing Computer Networks

Securing computer networks is essential to protect data, systems, and users from cyber threats. Key reasons include:

1. **Protects Sensitive Data –** Prevents theft or leakage of confidential information such as financial records, passwords, and personal details.
2. **Prevents Unauthorized Access –** Stops hackers or malicious users from entering the network.
3. **Ensures Business Continuity –** Avoids downtime and disruption caused by attacks like ransomware or DDoS.
4. **Maintains Trust –** Builds confidence among customers, employees, and partners by keeping systems safe.
5. **Compliance with Laws –** Meets legal and regulatory requirements for data protection.

Example:
A company with a secure firewall and intrusion detection system can block hackers from stealing customer credit card information.

5. Give two examples of secure communication methods.

Two examples of **secure communication methods** are:

1. **End-to-End Encrypted Messaging –** Apps like **Signal** or **WhatsApp** encrypt messages so only the sender and receiver can read them.
2. **Virtual Private Network (VPN) –** Encrypts internet traffic between your device and the VPN server, preventing eavesdropping.

Example:
Sending sensitive business documents through an **encrypted email service** like ProtonMail ensures no third party can read them in transit.

6. Define Privacy Guidelines.

Privacy Guidelines

Privacy guidelines are a set of rules, policies, and best practices designed to protect individuals' personal information from misuse, unauthorized access, or disclosure. They ensure that data is collected, stored, and shared responsibly and only for legitimate purposes.

Example:
A company following privacy guidelines will:

- Ask for user consent before collecting personal data.
- Store data securely using encryption.
- Share information only with authorized parties.

7. What is the main purpose of network security?

The main purpose of network security is **to protect the integrity, confidentiality, and availability of data and resources in a computer network** from unauthorized access, misuse, or attacks.

Key Points:

- **Confidentiality –** Ensures only authorized users can access sensitive information.
- **Integrity –** Prevents unauthorized changes or tampering with data.
- **Availability –** Keeps network services and resources accessible to legitimate users without disruption.

Example:
Using a firewall to block hackers from entering a company's internal network while allowing employees to work without interruptions.

8. State any two information security best practices.

Two **information security best practices** are:

1. **Use Strong and Unique Passwords –** Combine letters, numbers, and special characters, and avoid using the same password for multiple accounts.
2. **Regular Software Updates –** Keep operating systems, applications, and security software up to date to fix vulnerabilities.

Example:
Updating your web browser regularly prevents hackers from exploiting known security flaws.

Part-B (12 Marks – Long Answer)

1. Explain different types of cyber threats to personal computers and networks.

Types of Cyber Threats to Personal Computers and Networks

Cyber threats are malicious activities intended to damage, steal, or disrupt information and systems. Here are the main types:

1. Malware (Malicious Software)

- **Definition:** Software designed to harm or exploit computers.
- **Examples:** Viruses, worms, trojans, ransomware, spyware.
- **Impact:** Can delete files, steal personal information, or lock systems for ransom.

2. Phishing Attacks

- **Definition:** Fraudulent attempts to obtain sensitive data by pretending to be a trustworthy source (often via email or messages).
- **Impact:** Leads to identity theft, financial loss, and unauthorized access.

3. Denial of Service (DoS) and Distributed Denial of Service (DDoS)

- **Definition:** Overloading a network or website with traffic to make it unavailable to legitimate users.
- **Impact:** Service downtime, loss of revenue, reputational damage.

4. Man-in-the-Middle (MitM) Attacks

- **Definition:** An attacker secretly intercepts and possibly alters communication between two parties.
- **Impact:** Theft of login credentials, financial data, or private messages.

5. Password Attacks

- **Definition:** Attempts to crack or guess passwords through brute force, dictionary attacks, or social engineering.
- **Impact:** Unauthorized access to accounts and systems.

6. Insider Threats

- **Definition:** Malicious or careless actions by employees or trusted users.
- **Impact:** Data leaks, sabotage, or theft of intellectual property.

Example Scenario:A user downloads a “free” software that contains a **trojan**. The malware steals banking credentials, while a **phishing email** tricks them into giving away their password.

2. Discuss "Information Security Best Practices" in detail.

Information Security Best Practices

Information Security (InfoSec) best practices are **guidelines and strategies** followed to protect data, systems, and networks from unauthorized access, theft, or damage. They help ensure **confidentiality, integrity, and availability (CIA)** of information.

1. Use Strong and Unique Passwords

- **What to do:**
  - Minimum 8–12 characters.
  - Mix of uppercase, lowercase, numbers, and special characters.
  - Avoid personal details like birthdays or names.
- **Why:** Prevents brute force and dictionary attacks.
- **Example:** Instead of password123, use R@inB0w!Tree_93.

2. Enable Multi-Factor Authentication (MFA)

- **What to do:** Add a second verification step (OTP, fingerprint, authenticator app).
- **Why:** Even if the password is stolen, the account remains protected.
- **Example:** Gmail login with password + OTP sent to mobile.

3. Keep Software and Systems Updated

- **What to do:** Regularly install OS and application updates.
- **Why:** Updates fix security vulnerabilities.
- **Example:** Windows Update, antivirus definitions, browser updates.

4. Use Firewalls and Antivirus

- **What to do:** Enable network firewalls and install reputable antivirus software.
- **Why:** Blocks malicious traffic and detects harmful programs.
- **Example:** Windows Defender Firewall, Kaspersky, Bitdefender.

5. Backup Data Regularly

- **What to do:** Use offline or cloud backups.
- **Why:** Protects against ransomware, hardware failure, or accidental deletion.
- **Example:** Weekly backup to an external hard drive + Google Drive.

6. Beware of Phishing & Social Engineering

- **What to do:** Verify email senders, avoid clicking suspicious links, don't share confidential info.
- **Why:** Prevents identity theft and malware infections.
- **Example:** Avoid clicking on an email claiming "You've won a prize" with a strange link.

7. Secure Your Network

- **What to do:** Use WPA3/WPA2 encryption for Wi-Fi, change default router passwords.
- **Why:** Stops outsiders from intercepting your internet traffic.
- **Example:** Home Wi-Fi secured with a strong password instead of default admin123.

8. Limit User Access (Principle of Least Privilege)

- **What to do:** Give users only the permissions they need.
- **Why:** Reduces risk from compromised accounts.
- **Example:** Employees not needing admin rights shouldn't have them.

9. Encrypt Sensitive Data

- **What to do:** Use encryption tools for stored and transmitted data.
- **Why:** Keeps data unreadable to unauthorized users.
- **Example:** End-to-end encrypted messaging apps like Signal or WhatsApp.

10. Physical Security

- **What to do:** Lock devices, secure server rooms, use CCTV.
- **Why:** Prevents unauthorized physical access to systems.
- **Example:** Laptop auto-lock after 5 minutes of inactivity.

3. Explain privacy guidelines with real-time examples.

Privacy guidelines are **rules and recommended practices that help organizations and individuals protect personal and sensitive data from misuse, unauthorized access, and breaches**.
They ensure **data confidentiality, lawful processing, and user trust**.

Key Privacy Guidelines

1. **Data Minimization –** Collect only the information that is necessary.
   Example: An online shopping site asks for your delivery address but not your Aadhaar number.

2. **User Consent –** Always get permission before collecting or sharing personal data. *Example:* A mobile app requesting permission to access your location before using GPS services.
3. **Secure Data Storage –** Store data in encrypted formats to prevent unauthorized access. *Example:* A bank encrypting customer account details in its database.
4. **Access Control –** Limit data access to authorized personnel only. *Example:* Only HR staff having access to employee salary records.
5. **Transparency –** Clearly inform users how their data will be used. *Example:* Websites showing a "Privacy Policy" explaining what data is collected and why.
6. **Data Retention Policies –** Keep personal data only for as long as needed. *Example:* A job portal deleting applicant resumes after 6 months of inactivity.
7. **Regular Privacy Audits –** Check compliance with privacy laws and guidelines. *Example:* A healthcare organization conducting annual privacy audits to ensure HIPAA compliance.

In short: Privacy guidelines protect individuals' rights, maintain trust, and ensure compliance with laws like GDPR, HIPAA, and India's Digital Personal Data Protection Act (DPDPA).

4. Describe the process of securing computer networks.

Process of Securing Computer Networks

Securing a computer network means **protecting it from unauthorized access, misuse, damage, or disruption** while ensuring that legitimate users can use it without problems. The process generally involves the following steps:

1. Risk Assessment

- Identify network assets (servers, routers, switches, data).
- Find possible threats and vulnerabilities.
  Example: Detecting that the office Wi-Fi router uses a weak default password.

2. Implement Strong Access Controls

- Use strong passwords, two-factor authentication, and user account permissions.
  Example: Giving "admin" rights only to network administrators.

3. Use Firewalls and Intrusion Prevention Systems (IPS)

- Firewalls filter incoming and outgoing traffic based on security rules.
- IPS detects and blocks suspicious activities in real time.
  Example: Blocking traffic from blacklisted IP addresses.

4. Encrypt Data

- Use encryption for data **in transit** (SSL/TLS, VPN) and **at rest** (AES, BitLocker).
  Example: A company encrypting all employee emails.

5. Update and Patch Systems

- Regularly update operating systems, network devices, and applications to fix security holes.
  Example: Installing the latest Windows security patch to prevent ransomware attacks.

6. Monitor and Audit the Network

- Use tools like SIEM (Security Information and Event Management) to track unusual activity.
  Example: Detecting multiple failed login attempts from the same IP address.

7. Backup Data Regularly

- Keep multiple backups (local + cloud) for quick recovery after a cyberattack.
  Example: Daily backup of company database to a secure cloud server.

8. Educate Users

- Train employees and users to avoid phishing, suspicious downloads, and weak passwords.
  Example: Conducting quarterly cybersecurity awareness sessions.

5. Explain "Safe Internet Usage" in detail.

Safe Internet Usage

Safe Internet Usage means **using the internet responsibly and securely** to protect your personal information, devices, and online activities from cyber threats, while following legal and ethical rules. It's about **being careful, aware, and smart** when you browse, communicate, or share anything online.

➢ **Key Principles of Safe Internet Usage**

1. **Protect Your Personal Information**
   - Never share sensitive data (like bank details, passwords, or Aadhaar number) on unsafe websites or with unknown people.
   - Check if a website is secure (look for "https://" and a padlock icon).
     Example: Entering credit card details only on secure e-commerce sites like Amazon or Flipkart.
2. **Use Strong Passwords & Two-Factor Authentication (2FA)**
   - Create passwords with a mix of letters, numbers, and symbols.

- Use 2FA to add an extra layer of security.
  Example: Gmail sending you an OTP before logging in from a new device.

3. **Beware of Phishing & Scams**
   - Do not click on suspicious links in emails, SMS, or social media.
   - Verify sender identity before downloading attachments.
     Example: Ignoring an email claiming "You've won $1 million" and asking for bank details.
4. **Keep Devices & Software Updated**
   - Regularly update your operating system, browsers, and apps to fix security flaws.
   - Use antivirus software.
     Example: Updating Windows to protect against ransomware like WannaCry.
5. **Avoid Using Public Wi-Fi Without Protection**
   - Use a **VPN** (Virtual Private Network) when connecting to public Wi-Fi.
   - Avoid logging into banking accounts on public networks.
     Example: Using a VPN app when working in a coffee shop.
6. **Download Only from Trusted Sources**
   - Get apps from official stores (Google Play Store, Apple App Store).
   - Avoid pirated software and cracked versions.
     Example: Installing Microsoft Office from the official Microsoft website.
7. **Be Careful on Social Media**
   - Limit what you share publicly (location, personal life details).
   - Adjust privacy settings.
     Example: Keeping your Facebook profile visible only to friends.
8. **Think Before You Click**
   - Check links before opening.
   - Avoid pop-up ads claiming free prizes.
     Example: Hovering over a link to see the real destination before clicking.

➢ **Real-Time Examples of Unsafe Internet Use & Consequences**

Unsafe Action	**Possible Threat**
Clicking on unknown email links	Phishing attack, account theft

Using "123456" as a password	Easy hacking
Downloading pirated movies	Malware infection, legal action
Sharing vacation plans publicly	Risk of burglary

- **Best Practices for Safe Internet Usage**

Practice	**Why it's important**
Use HTTPS websites	Encrypts your data
Enable firewall	Blocks suspicious traffic
Backup data regularly	Recover from cyberattacks
Educate yourself	Stay updated on cyber threats

6. Write about secure communication protocols with examples.

Secure Communication Protocols

Secure communication protocols are special rules and procedures used to protect data while it is being transmitted over a network. These protocols ensure that the data remains **confidential, intact, and accessible only to authorized parties**.

Key Goals of Secure Communication Protocols

- **Confidentiality –** Data is encrypted so that unauthorized people cannot read it.
- **Integrity –** Prevents data from being modified during transmission.
- **Authentication –** Verifies the identity of the sender and receiver.
- **Non-repudiation –** Ensures that a sender cannot deny sending a message.

Common Secure Communication Protocols and Examples

a) HTTPS (Hypertext Transfer Protocol Secure)

- Used for secure web browsing.
- Encrypts data between the browser and the website using SSL/TLS.
- **Example:** Banking websites, e-commerce transactions.

b) SSL/TLS (Secure Sockets Layer / Transport Layer Security)

- Provides encryption for internet communication.
- Works with various applications like email, VoIP, and instant messaging.
- **Example:** Gmail uses TLS to secure emails in transit.

c) S/MIME (Secure/Multipurpose Internet Mail Extensions)

- Encrypts and digitally signs email messages.
- Ensures privacy and authenticity of emails.
- **Example:** Corporate email systems for confidential communication.

d) IPsec (Internet Protocol Security)

- Works at the network layer to encrypt and authenticate IP packets.
- Often used in VPNs (Virtual Private Networks).
- **Example:** Remote employees securely connecting to a company's network.

e) SSH (Secure Shell)

- Secure method to remotely access and manage servers.
- Encrypts commands and data sent over the network.
- **Example:** System administrators managing cloud servers securely.

Real-World Example

When you shop online, **HTTPS** ensures that your credit card information is encrypted during the transaction, preventing hackers from stealing your details.

7. Explain the importance of protecting your computer and its contents.

Protecting your computer and its data is essential because modern computers store a wide range of **personal, financial, professional, and sensitive information**. If left unprotected, this information can be stolen, destroyed, or misused, leading to **financial loss, identity theft, privacy invasion, or system damage**.

✓ **Reasons Why Protection is Important**

a) Preventing Data Loss

- Important documents, photos, and project files can be lost due to malware, accidental deletion, or hardware failure.
- **Example:** A virus corrupting all your college assignments or office reports.

b) Protecting Personal Information

- Hackers can steal personal details like name, address, Aadhaar number, or bank credentials.
- **Example:** Phishing attacks stealing credit card information from online users.

c) Avoiding Financial Loss

- Cybercriminals can misuse your bank accounts, credit cards, or online wallets if your computer is not secure.
- **Example:** Ransomware attacks demanding money to unlock files.

d) Maintaining Privacy

- Without protection, hackers can track your activities, capture your keystrokes, or turn on your webcam without permission.
- **Example:** Spyware recording your personal conversations.

e) Ensuring Business Continuity

- In organizations, data breaches can halt operations, damage reputation, and lead to legal consequences.
- **Example:** An unprotected company server leaking customer data to competitors.

✓ **Ways to Protect Your Computer**

1. **Use antivirus and anti-malware software** to detect and remove threats.
2. **Enable firewalls** to block unauthorized access.
3. **Regularly update operating systems and software** to patch security vulnerabilities.
4. **Use strong passwords** and enable multi-factor authentication.
5. **Backup data** regularly to an external drive or cloud storage.

Real-World Example

In 2017, the **WannaCry ransomware attack** infected over **200,000 computers** in 150 countries, encrypting files and demanding payment. Many victims could have avoided it by keeping their systems updated with the latest security patches.

8. Discuss basics of networking relevant to cyber security.

Basics of Networking Relevant to Cyber Security

Networking forms the backbone of communication between computers, devices, and servers. In **cyber security**, understanding the basics of networking is crucial because most attacks, threats, and defenses operate over networks.

1. What is Computer Networking?

A **computer network** is a collection of interconnected devices (computers, servers, routers, switches, etc.) that share data and resources.

- **Example:** The internet, a local office network (LAN), or a home Wi-Fi network.

2. Key Networking Concepts in Cyber Security

a) IP Address & MAC Address

- **IP Address**: A unique logical identifier for a device on a network (e.g., 192.168.1.5).
- **MAC Address**: A unique hardware address assigned to a network card (e.g., 00:1A:2B:3C:4D:5E).
- **Cyber Security Relevance:** IPs help trace network activity, while MAC addresses help identify specific devices.

b) Types of Networks

1. **LAN (Local Area Network) –** Small area like an office.
2. **WAN (Wide Area Network) –** Large area, e.g., the internet.
3. **MAN (Metropolitan Area Network) –** Covers a city.
4. **PAN (Personal Area Network) –** Small range, e.g., Bluetooth.

- **Cyber Security Relevance:** Different network types have different vulnerabilities; e.g., Wi-Fi hacking is common in LANs.

c) Protocols

Protocols define how data is transmitted. Common ones:

- **TCP/IP –** The foundation of internet communication.
- **HTTP/HTTPS –** For web browsing (HTTPS is secure).
- **FTP/SFTP –** For file transfers (SFTP is secure).
- **SMTP/IMAP/POP3 –** For emails.

- **Cyber Security Relevance:** Secure versions (HTTPS, SFTP, SMTPS) protect against eavesdropping.

d) Ports and Services

- **Ports**: Virtual doorways for specific types of network communication (e.g., Port 80 for HTTP, Port 443 for HTTPS).
- **Cyber Security Relevance:** Open ports can be exploited; port scanning is a common hacking technique.

e) Firewalls and Intrusion Detection Systems (IDS)

- **Firewall:** Filters incoming and outgoing traffic based on rules.
- **IDS:** Monitors for suspicious activity.
- **Cyber Security Relevance:** First line of defense against unauthorized access.

f) DNS (Domain Name System)

- Converts domain names (like google.com) into IP addresses.
- **Cyber Security Relevance:** DNS hijacking can redirect users to malicious sites.

3. Networking Threats in Cyber Security

- **Phishing:** Fake websites to steal data.
- **Man-in-the-Middle (MITM) Attacks:** Intercepting communication.
- **DDoS (Distributed Denial of Service):** Flooding a network with traffic to crash it.
- **Packet Sniffing:** Capturing unencrypted data packets.

4. Importance of Networking Knowledge for Cyber Security

- Helps identify and trace cyber-attacks.
- Enables configuration of secure systems.
- Helps understand attacker methods like port scanning, IP spoofing, and DNS attacks.
- Assists in implementing secure protocols and firewalls.

UNIT – II: Ethics in Cyber Security & Cyber Law

Part-A (2 Marks – Short Answer)

1. Define Cyber Law.

Cyber Law: Cyber Law refers to the set of laws, rules, and regulations that govern the use of the internet, digital devices, and online communication. It deals with issues such as cybercrimes, online privacy, intellectual property rights, electronic transactions, and data protection.

Example:
In India, the **Information Technology Act, 2000 (IT Act)** is the main cyber law that addresses offenses like hacking, identity theft, and online fraud.

2. What is meant by "Fair Use" in cyber security?

Fair Use in Cyber Security

Fair Use refers to the legal principle that allows limited use of copyrighted digital material **without the permission of the copyright owner**, for purposes such as education, research, criticism, commentary, or news reporting.

In cyber security, fair use is important when accessing, sharing, or reproducing digital content — ensuring that such use does not violate copyright laws.

Example:
A teacher showing a short clip of a cybersecurity documentary in a classroom for educational purposes is considered **fair use**, but uploading the full movie online for public download is **not**.

3. Define Intellectual Property.

Intellectual Property (IP)

Intellectual Property refers to **creations of the mind —** such as inventions, artistic works, designs, symbols, names, and images — that are legally protected from unauthorized use by others.

It gives the creator **exclusive rights** to use, produce, or sell their creation for a certain period.

Examples in Cyber Security:

- Software programs (protected by copyright or patents)
- Company logos (protected by trademarks)
- Unique algorithms or encryption techniques (protected by patents/trade secrets)

4. Give an example of a cybercrime.

Example of a Cybercrime:

Phishing Attack – Sending fake emails pretending to be from a bank to trick people into giving their login credentials or credit card information.

5. What is Ethical Hacking?

Ethical Hacking: Ethical hacking is the authorized practice of intentionally probing computer systems, networks, or applications to identify security vulnerabilities and fix them before malicious hackers can exploit them. Ethical hackers work with permission and follow legal guidelines.

Example: A company hires a security expert to test its website for weaknesses and provide solutions to strengthen security.

6. Mention any two types of electronic evidence.

Two types of electronic evidence:

1. **Emails –** Messages, attachments, and metadata that can be used as proof in investigations.
2. **Digital Documents –** Files such as PDFs, Word documents, or spreadsheets stored on computers or cloud systems.

7. Define Freedom of Speech in the context of cyber space.

Freedom of Speech in the context of cyberspace: It is the right of individuals to express their opinions, ideas, and information through the internet or other digital platforms without censorship or undue restriction, while respecting laws related to hate speech, defamation, and national security.

8. List two types of internet fraud.

Two types of internet fraud:

1. **Phishing –** Sending fake emails or messages to trick people into sharing sensitive information like passwords or bank details.
2. **Online Auction Fraud –** Misrepresenting products or failing to deliver items after payment on e-commerce or auction sites.

Part-B (12 Marks – Long Answer)

1. **Discuss privacy and intellectual property in cyber security.**

1. Privacy in Cyber Security
Privacy refers to the right of individuals and organizations to keep their personal, sensitive, or confidential data safe from unauthorized access, misuse, or disclosure.

- **Importance:** Protects against identity theft, fraud, and misuse of personal data.
- **Examples in Real Time:**
  - Social media platforms allowing users to control who sees their posts.
  - Encrypted messaging apps like **Signal** and **WhatsApp** to keep conversations private.
- **Best Practices for Privacy:**
  - Use strong passwords and two-factor authentication.
  - Limit sharing of personal data online.
  - Regularly update privacy settings on websites and apps.

2. Intellectual Property (IP) in Cyber Security

Intellectual Property refers to creations of the mind, such as inventions, literary works, designs, symbols, or software, that are legally protected from unauthorized use.

- **Types of IP:**
    1. **Copyrights –** Protect books, software, music, videos.
    2. **Patents –** Protect inventions and technical solutions.
    3. **Trademarks –** Protect brand names, logos, and symbols.
    4. **Trade Secrets –** Protect confidential business information.
- **Importance in Cyber Security:** Prevents piracy, plagiarism, and software theft.
- **Examples in Real Time:**
    - Microsoft suing a company for pirated Windows software.
    - A movie studio taking legal action against illegal torrent sites.

In short:

- **Privacy** protects personal data.
- **Intellectual Property** protects creative and innovative work.

2. Explain professional ethics in cyber security with examples.

Professional Ethics in Cyber Security

Definition:

Professional ethics in cyber security refers to the moral principles, standards, and guidelines that govern how cyber security professionals should behave while performing their duties. It ensures that they act with honesty, integrity, and responsibility to protect systems, data, and users from harm.

Key Principles of Professional Ethics in Cyber Security

1. **Integrity and Honesty –** Never mislead clients or employers; provide truthful reports on security findings.
2. **Confidentiality –** Keep sensitive data secret unless authorized to disclose it.
3. **Non-Maleficence (Do No Harm) –** Ensure that actions do not intentionally or negligently harm systems or individuals.
4. **Competence –** Only perform tasks for which you are qualified and keep skills updated.

5. **Respect for Law –** Follow cyber laws and regulations while performing security tasks.

Examples in Real Life

- **Example 1:** A penetration tester discovers a vulnerability in a bank's server.
    - Ethical behavior: Report the issue to the bank without exploiting it for personal gain.
    - Unethical behavior: Selling the vulnerability details on the dark web.
- **Example 2:** A network administrator finds confidential salary data.
    - Ethical behavior: Keep it private and use it only for authorized purposes.
    - Unethical behavior: Sharing it with other employees or online.
- **Example 3:** A cyber security consultant is hired to assess a company's security.
    - Ethical behavior: Conduct only agreed-upon tests and follow the scope.
    - Unethical behavior: Access personal email accounts of employees without permission.

In short:

Professional ethics ensures cyber security experts protect data, respect privacy, follow laws, and avoid actions that could harm individuals or organizations.

3. Write about trademarks and their importance in cyber law.

Trademarks and Their Importance in Cyber Law

Definition of Trademark

A **trademark** is a symbol, word, phrase, logo, design, or combination of these that identifies and distinguishes the goods or services of one business from others.
Example: *Apple logo*, *Nike's "Swoosh"*, *Google's name in a specific font*.

Trademarks in Cyber Law

In the digital world, trademarks are also protected under **cyber law** to prevent:

- **Cybersquatting –** Registering domain names similar to famous trademarks to profit from selling them back.
- **Trademark Infringement –** Using a brand's logo, name, or domain without permission to mislead users.
- **Counterfeiting –** Selling fake products online using a company's brand identity.

Cyber law ensures that online businesses and e-commerce platforms cannot misuse registered trademarks.

Importance of Trademarks in Cyber Law

1. **Brand Protection –** Safeguards a company's reputation and prevents misuse of its identity.
2. **Consumer Trust –** Helps customers identify genuine products/services in the digital marketplace.
3. **Legal Ownership –** Gives the trademark owner exclusive rights to use and control its usage.
4. **Prevention of Fraud –** Stops cybercriminals from deceiving customers using fake branding.
5. **Global Recognition –** Protects brand identity across countries in online business.

Example

If someone registers the domain **"amazonn-sale.com"** and uses Amazon's logo to scam customers, it violates trademark rights. Under cyber law, Amazon can take legal action to remove the site and claim damages.

4. Describe various types of internet fraud with examples.

Types of Internet Fraud with Examples

1. Phishing

- **Meaning:** Fraudulent attempts to obtain sensitive information (passwords, bank details) by pretending to be a trusted entity.
- **Example:** Receiving an email that looks like it's from your bank, asking you to "verify" your account by clicking a fake link.

2. Identity Theft

- **Meaning:** Stealing someone's personal information to commit fraud or crimes.
- **Example:** Using stolen Aadhaar or credit card details to make online purchases.

3. Online Shopping Fraud

- **Meaning:** Fake e-commerce websites selling products that never get delivered or delivering poor-quality items.
- **Example:** A website offering branded shoes at 90% discount, but sending cheap imitations or nothing at all.

4. Advance Fee Fraud

- **Meaning:** Asking for upfront payment with the promise of large returns that never materialize.
- **Example:** "Lottery winnings" emails asking for processing fees before releasing the prize.

5. Auction Fraud

- **Meaning:** Misrepresenting products in online auctions or not delivering them after payment.
- **Example:** Selling a "new" laptop on eBay but delivering an old or non-working one.

6. Credit Card Fraud

- **Meaning:** Unauthorized use of someone's credit/debit card information for transactions.
- **Example:** Skimming card data and using it for online shopping without the owner's consent.

5. Explain cybercrimes and their classification.

Cybercrimes and Their Classification

Definition of Cybercrime

Cybercrime refers to **illegal activities carried out using computers, networks, or the internet** as a tool, target, or both.
It includes activities that harm individuals, organizations, or governments through data theft, fraud, disruption, or unauthorized access.

Classification of Cybercrimes

1. Crimes Against Individuals

- Target a person's data, identity, or privacy.
- **Examples:**
    - Identity theft (stealing personal details)
    - Cyberstalking (harassing someone online)
    - Phishing (tricking to reveal passwords)
    - Defamation via social media posts

2. Crimes Against Property

- Target digital assets like data, software, and systems.

- **Examples:**
    - Hacking into systems
    - Malware attacks destroying data
    - Intellectual property theft (pirated software, music, movies)
    - Ransomware (locking files and demanding payment)

3. Crimes Against Government / Society

- Target government systems or public infrastructure, affecting national security.
- **Examples:**
    - Cyberterrorism (attacking power grids, defense systems)
    - Website defacement of government portals
    - Spreading fake news to cause panic
    - Denial-of-Service (DoS) attacks on critical services

6. Discuss the role of cyber laws in India.

Role of Cyber Laws in India

Introduction

Cyber laws in India are legal frameworks designed to regulate activities in **cyberspace**—covering the internet, computers, digital devices, and electronic communication.
They protect individuals, organizations, and the government from cybercrimes, ensure safe e-commerce transactions, and safeguard privacy.

The **Information Technology Act, 2000 (IT Act)** is the primary law governing cyber activities in India, later amended in **2008** to address new threats.

Key Roles of Cyber Laws in India

1. Preventing and Punishing Cybercrimes

- Defines various cyber offences such as hacking, phishing, cyberstalking, identity theft, and cyberterrorism.
- Specifies **penalties** and **punishments** to deter offenders.
- **Example:** Section 66 of IT Act – covers hacking with imprisonment up to 3 years and/or fine.

2. Regulating E-Commerce and Digital Transactions

- Provides **legal recognition** for electronic records and digital signatures.

- Facilitates secure online contracts, banking, and business.
- **Example:** Online agreements signed digitally are legally valid under the IT Act.

3. Protecting Privacy and Data Security

- Ensures protection of sensitive personal data and financial information.
- Mandates security practices for companies handling user data.
- **Example:** Section 43A – organizations are liable to pay compensation for negligence in securing data.

4. Supporting Law Enforcement

- Gives investigative powers to police and cyber cells.
- Allows tracking, interception, and seizure of digital evidence for legal proceedings.

5. Safeguarding Intellectual Property Online

- Protects copyrights, trademarks, and patents in the digital space.
- Helps combat software piracy, illegal downloads, and brand misuse.

6. Securing Critical Infrastructure

- Addresses cyberterrorism and attacks on national security systems.
- **Example:** Section 66F – covers cyberterrorism with imprisonment up to life.

7. Explain the concept of electronic evidence and its legal value.

➢ **Concept of Electronic Evidence**

Definition:
Electronic evidence refers to any information stored or transmitted in a digital form that can be presented in a court of law as proof in a legal case.
It is also called **Digital Evidence**.

Sources of Electronic Evidence:

- Computers & laptops
- Mobile phones & tablets
- Email servers
- CCTV systems
- Cloud storage services
- Social media platforms

➢ **Examples of Electronic Evidence**

1. **Emails –** Communication records (e.g., phishing scam emails).
2. **Chat logs –** Messages from WhatsApp, Telegram, or Messenger.
3. **Digital documents –** PDF contracts, scanned agreements.
4. **Multimedia files –** Photos, videos, or audio recordings.
5. **Transaction records –** Online banking logs, cryptocurrency transactions.
6. **Web server logs –** IP addresses, login attempts, and browsing history.

➢ **Importance & Legal Value**

a. Admissibility in Court

- In India, the **Indian Evidence Act, 1872 (Section 65B)** governs the admissibility of electronic records.
- The evidence must be **authentic**, **reliable**, and **untampered**.
- Requires a **certificate under Section 65B** for court acceptance.

b. Benefits in Legal Investigations

- **Accuracy:** Provides exact records of events.
- **Timeline building:** Helps reconstruct crime sequences.
- **Proof of intent:** Shows communication or transaction trails.
- **Wide coverage:** Can link suspects, victims, and crime scenes.

4. Challenges in Using Electronic Evidence

- **Data tampering:** Easily editable or deletable.
- **Authentication issues:** Difficulty proving origin and integrity.
- **Jurisdiction problems:** Servers may be in another country.
- **Privacy concerns:** Must follow legal procedures during data collection.

5. Real-World Example

- In a **cyber fraud case**, bank server logs showing unauthorized online transfers from the victim's account were presented as **electronic evidence**.
- Under Section 65B, the bank provided a certificate verifying the logs' authenticity.
- The court accepted this as proof and convicted the offender.

8. Discuss ethical hacking and its types.

What is Ethical Hacking?

Definition:
Ethical hacking is the authorized practice of bypassing system security to identify vulnerabilities, threats, or weaknesses in a computer system, network, or application **before malicious hackers exploit them**.

Ethical hackers work **with permission** to protect systems.

Key Points:

- Also called **White Hat Hacking**.
- Objective is **protection**, not harm.
- Involves **penetration testing** and **vulnerability assessment**.
- Requires **legal authorization** from the system owner.

Role of an Ethical Hacker

- Simulate cyberattacks to test defenses.
- Identify weaknesses in applications, networks, or devices.
- Suggest fixes to improve security.
- Ensure compliance with cybersecurity standards.

Legal and Ethical Side

- **Legal** if done with permission (e.g., by security teams, consultants).
- **Illegal** if done without consent, even with good intentions.
- Governed by laws like the **IT Act, 2000** in India

Types of Ethical Hacking

a. Web Application Hacking

- **Target:** Websites and web-based services.
- **Goal:** Find vulnerabilities like SQL Injection, XSS, broken authentication.
- **Example:** Testing a bank's online portal for security loopholes.

b. Network Hacking

- **Target:** Wired and wireless networks.
- **Goal:** Identify weaknesses in network devices (routers, firewalls, switches).
- **Example:** Checking if an organization's Wi-Fi uses weak encryption.

c. System Hacking

- **Target:** Operating systems and individual computers.
- **Goal:** Gain unauthorized access by exploiting OS flaws, weak passwords.
- **Example:** Attempting to log in as an admin by cracking the password.

d. Social Engineering

- **Target:** Human psychology instead of technology.
- **Goal:** Trick people into revealing sensitive data.
- **Example:** Phishing emails that pretend to be from HR asking for login credentials.

e. Mobile Application Hacking

- **Target:** Android/iOS apps.
- **Goal:** Find security gaps in mobile apps.
- **Example:** Testing a shopping app for insecure payment gateway integration.

f. Wireless Network Hacking

- **Target:** Wi-Fi networks.
- **Goal:** Detect insecure configurations, weak passwords, or outdated protocols.
- **Example:** Breaking into a network using WPA2 handshake cracking.

Difference Between Ethical & Malicious Hacking

Aspect	Ethical Hacking	Malicious Hacking
Permission	Legal, with consent	Illegal, without consent
Purpose	Security improvement	Data theft, disruption
Outcome	Increases security	Damages security
Example	Penetration testing	Ransomware attack

Real-Life Example

- **Case:** In 2021, an ethical hacker reported a bug in Facebook's login system that could allow account takeover.
- **Result:** Facebook patched the bug and rewarded the hacker with **$50,000** under its **Bug Bounty Program**.