## **UNIT 1: Introduction to Cyber Security and Cybercrime**

### 1. Cybersecurity vs Cybercrime

* **Cybersecurity**: Protects systems, networks, and data.
* **Cybercrime**: Illegal acts using digital devices/internet.

### 2. Origin of Cybercrime

* “Cyber” from Greek kybernetes = steersman/governor.
* Early cybercrimes: Hacking, online fraud.
* Modern threats: Ransomware, identity theft, espionage.

### 3. Information Security & CIA Triad

* **Confidentiality**: Only authorized access.
* **Integrity**: Data is correct and unchanged.
* **Availability**: Data/services are always accessible.

### 4. Types of Cybersecurity

1. **Network Security** – Blocks intrusions/malware.
2. **Information Security** – Protects data from leaks.
3. **Application Security** – Secures software from threats.
4. **Cloud Security** – Protects cloud services.
5. **Operational Security** – Secures decision-making/data flow.
6. **Endpoint Security** – Protects end devices.
7. **IoT Security** – Secures smart devices.
8. **Cryptography** – Encrypts data in storage and transit.

### 5. Types of Cybercriminals

1. **Hackers**: White-hat (ethical) / Black-hat (malicious).
2. **Script Kiddies**: Inexperienced attackers.
3. **Cyber Terrorists**: Cause panic/infrastructure harm.
4. **State-Sponsored Hackers**: Government-backed attacks.
5. **Insider Threats**: Disloyal employees.
6. **Hacktivists**: Protest via hacking.

### 6. Classifications of Cybercrime

1. **Against Individuals**:
   * Identity theft, stalking, harassment.
2. **Against Organizations**:
   * Data breaches, phishing, ransomware.
3. **Against Governments**:
   * Espionage, cyber warfare, terrorism.

### 7. Categories by Method

* Financial fraud
* Cyber espionage
* Phishing & social engineering
* Hacking
* Malware attacks
* Cyberbullying

## ✅ **UNIT 2: Cyber Laws & Legal Perspectives**

### 1. Indian Cyber Laws

* Governed by **IT Act, 2000** (amended in 2008).
* Key aims:
  + Prevent cybercrimes
  + Legalize e-transactions & signatures
  + Regulate hacking, privacy, fraud

### 2. IT Act, 2000 (Amendments 2008)

* **66A**: Offensive messages online (now repealed).
* **43A**: Data protection obligations.
* **66F**: Defines & penalizes cyberterrorism.
* Covers: Identity theft, phishing, data breaches.

### 3. International Child Protection Laws

* **COPPA** (1998): Parental consent for child data.
* **CIPA** (2000): Filters inappropriate content in schools.
* **Sexual Predator Laws**:
  + Penalize child grooming, abuse.
* **COPA** (1998): Ban harmful content (now invalid).
* **CDA – Section 230**:
  + Protects platforms from liability for user content.

### 🔹 4. Intellectual Property in Cyberspace

1. **Copyright** – Digital work protection (DMCA).
2. **Patent** – Software, tech inventions.
3. **Trademark** – Brand identity protection.
4. **Trade Secret** – Confidential business info.
5. **Trade Name** – Business name rights.
6. **Domain Name** – Prevent cybersquatting (ICANN).

### 🔹 5. Global Response to Cybercrime

* **Budapest Convention**: First cybercrime treaty.
* **INTERPOL/Europol**: Global coordination.
* **GDPR (EU)**: Data privacy and security law.
* **MLATs**: International investigation cooperation.

### 🔹 6. Legal Implications

* Penalties: Fines, jail, company liability.
* Offenses: Fraud, hacking, harassment, negligence.

### 🔹 7. Compliance & Regulatory Frameworks

* **GDPR** – EU privacy law.
* **HIPAA** – US health data security.
* **ISO 27001** – InfoSec standards.
* **PCI-DSS** – Payment data protection

**UNIT 3**

**1. Proxy Server**

* **Definition**: A middleman between user and the internet.
* **How it works**:
  + User request → proxy server → website → proxy → user.
* **Why use it**:
  + **Personal Use**:
    - Hide IP
    - Bypass regional blocks
    - Private browsing
  + **Company/School Use**:
    - Block/filter content
    - Save data (cache)
    - Monitor usage
* **Security Help**:
  + Works like firewall
  + IP masking
  + Threat scanning
  + Encryption
* **Advantages**:
  + IP hiding, geo-bypass, speed boost (cache), content filtering, low cost
* **Disadvantages**:
  + No strong encryption
  + Limited security

**2. Anonymizers**

* **Definition**: Tools/services for full anonymity online
* **How it works**:
  + Routes data through random servers
  + Example: Tor, VPN
* **Use Cases**:
  + Private browsing
  + Dark web access
  + Criminal activities
* **Comparison (Proxy vs. Anonymizer)**:
  + IP hiding: Yes vs. Fully
  + Encryption: Weak vs. Strong
  + Anonymity: Medium vs. High
* **Advantages**:
  + Strong privacy & encryption
  + Public Wi-Fi safety
  + Anti-tracking & censorship bypass
* **Disadvantages**:
  + Slower speed
  + Website blocking (Tor)
  + Cost (VPN)

**3. Password Cracking**

* **Definition**: Gaining unauthorized access by cracking passwords
* **Types**:
  + **Brute Force**:
    - Tries every combo
    - Accurate but time-consuming
  + **Dictionary Attack**:
    - Uses common passwords list
    - Fast, but ineffective for strong passwords
  + **Rainbow Table**:
    - Uses precomputed hash tables
    - Fast lookup, but large storage & weak vs. salted hashes
* **Legitimate Uses**:
  + Password recovery
  + Security testing
* **Illegal Uses**:
  + Unauthorized access, identity theft
* **Protection**:
  + Strong passwords
  + Multi-factor authentication
  + Password managers
  + Hashing + salting

**4. Keyloggers**

* **Definition**: Records keystrokes to capture private info
* **Types**:
  + **Software**: Hidden malware
  + **Hardware**: Physical device
* **Data captured**:
  + Passwords, chats, usernames
* **Real Example**: 2017 HP laptops had hidden keylogger
* **Dangers**:
  + Identity theft, privacy loss, blackmail
* **Protection**:
  + Antivirus
  + Avoid unknown downloads
  + Keep OS updated

**5. Spyware**

* **Definition**: Secretly monitors user activity
* **Data Collected**:
  + Browsing, emails, login info, webcam/audio
* **Types**:
  + Adware
  + System Monitors
  + Trojans
  + Tracking Cookies
* **Entry Methods**:
  + Free software, fake links, emails
* **Protection**:
  + Antivirus, careful downloading, system updates, 2FA

**6. Steganography**

* **Definition**: Hiding data inside images/videos/etc.
* **Techniques**:
  + LSB, metadata injection, invisible text
* **Uses**:
  + Journalists, copyright, encryption
* **Risks**:
  + Criminal misuse, hard to detect
* **Detection**:
  + Steganalysis, hashing, metadata checks

**7. DoS and DDoS Attacks**

* **DoS**: Overloads server from one source
* **DDoS**: Multiple devices attack simultaneously
* **How it works**:
  + Flood traffic → server crash
* **Tools**:
  + Botnets, LOIC
* **Risks**:
  + Illegal, service disruption, revenue loss
* **Protection**:
  + Firewall, CDN, anti-DDoS tools

**8. SQL Injection**

* **Definition**: Injecting SQL code into input fields
* **Effects**:
  + Bypass login, steal/modify/delete data
* **Prevention**:
  + Prepared statements
  + Input validation
  + Web Application Firewall (WAF)
  + Limited DB permissions
  + Error handling

**9. Wireless Network Attacks**

* **Types**:
  + Eavesdropping
  + MITM
  + Rogue Access Points
  + DoS
* **Protection**:
  + WPA3, VPN, strong passwords, disable WPS

**10. Phishing**

* **Definition**: Tricking people into revealing info
* **Method**:
  + Fake emails/SMS → fake links → data theft
* **Protection**:
  + Avoid suspicious links
  + MFA
  + Anti-phishing tools

**11. Identity Theft**

* **Definition**: Misusing someone’s personal data
* **Method**:
  + Phishing, data breach, social engineering
* **Impact**:
  + Financial fraud, unauthorized accounts
* **Protection**:
  + Monitor accounts, strong passwords, credit freezes

**UNIT 4**

**1. Types of Cyberattacks**

* **Phishing**: Tricking users into giving up information.
* **Ransomware**: Encrypting data and demanding ransom.
* **Denial of Service (DoS)**: Flooding servers to crash them.
* **Malware**: Malicious software for data theft/damage.

**2. Phishing**

* **Definition**: Fake messages to steal credentials.
* **Method**:
  + Impersonation (bank, company)
  + Fake links/attachments
* **Consequences**:
  + Identity theft
  + Financial loss
  + Reputation damage

**3. Ransomware**

* **Definition**: Malware that locks data and demands payment.
* **Method**:
  + Spread via email, malicious links
  + Encrypts data, shows ransom message
* **Consequences**:
  + Permanent data loss
  + Financial damage
  + Public trust issues

**4. DoS (Denial of Service)**

* **Definition**: Flooding a server to make it unavailable.
* **Method**:
  + Overloads with traffic
  + System crashes or becomes slow
* **Consequences**:
  + Downtime
  + Revenue loss
  + User frustration

**5. Malware**

* **Definition**: Software made to harm systems.
* **Types**:
  + Virus
  + Trojan
  + Worm
  + Spyware
* **Consequences**:
  + Data theft
  + System crashes
  + Financial harm

**6. Social Engineering**

* **Definition**: Manipulating people to reveal confidential data.
* **Types**:
  1. **Phishing**
  2. **Spear Phishing** – Targeted
  3. **Pretexting** – False identity
  4. **Baiting** – Enticing offers
  5. **Quizzes & Surveys** – Data mining
  6. **Impersonation** – Physical or digital
* **Why it works**:
  1. Exploits trust, urgency, curiosity

**7. Cyber Stalking**

* **Definition**: Online harassment or tracking
* **Tactics**:
  + Repeated messages
  + Monitoring activities
  + Impersonation
* **Effects**:
  + Psychological harm
  + Privacy loss
  + Relationship/work impact
* **Protection**:
  + Privacy settings
  + Report threats
  + Legal action

**8. Cybercafés and Cybercrimes**

* **Definition**: Public internet access centers
* **Criminal Use**:
  + Hacking
  + Identity theft
  + Malware spreading
* **Challenges**:
  + Lack of monitoring
  + Anonymity
* **Protection**:
  + Avoid sensitive work
  + Use VPNs
  + Clear browser data

**9. Botnets**

* **Definition**: Network of infected devices controlled by a hacker
* **Working**:
  + Infection → Control via C&C server → Execution
* **Uses**:
  + DDoS
  + Spam
  + Credential stuffing
* **Protection**:
  + Antivirus/firewall
  + Strong passwords
  + Monitor traffic

**10. Attack Vectors**

* **Definition**: Pathway attackers use to gain access
* **Examples**:
  + Phishing
  + Malware
  + SQL Injection
  + MitM
  + Social engineering
  + RDP Attacks
  + Drive-by Downloads
  + Insider threats

**11. Cloud Computing**

* **Definition**: Providing IT services over the internet
* **Models**:
  + **IaaS**: Infrastructure (e.g., AWS)
  + **PaaS**: Developer tools/platform (e.g., Heroku)
  + **SaaS**: Ready software (e.g., Google Drive)
  + **FaaS**: Function-based execution (e.g., AWS Lambda)

**UNIT 5**

**1. Cost of Cybercrimes**

* **Types of Costs**:
  + Direct financial loss
  + Reputation damage
  + Penalties & fines
  + Operational disruption
  + Legal/litigation costs
* **Preventive Measures**:
  + Cybersecurity tools (firewalls, encryption)
  + Employee training
  + Cyber insurance

**2. Intellectual Property Rights (IPR) Issues**

* **Definition**: Legal rights over original creations
* **Types of IPR Violations**:
  + **Copyright Infringement**: Using music, movies, software illegally
  + **Patent Violations**: Using unlicensed inventions
  + **Trademark Violations**: Using fake logos/brands
  + **Trade Secret Theft**: Leaking formulas/business data
  + **Counterfeiting**: Selling fake goods
* **Challenges**:
  + Easy digital copying
  + International jurisdiction limits
  + Weak enforcement

**UNIT 5 (continued)**

**3. IPR (Intellectual Property Rights) Protection Strategies**

* **Clear Documentation**:
  + Keep detailed records of your work (e.g., inventions, code, art).
* **Registering IP**:
  + File for patents, copyrights, and trademarks to strengthen legal rights.
* **Confidentiality Agreements**:
  + Use NDAs with employees, vendors, or partners.
* **Monitoring and Enforcement**:
  + Monitor for infringement, take legal action (e.g., cease-and-desist).
* **Cybersecurity Measures**:
  + Encrypt data, limit access, use firewalls to protect IP.
* **Licensing and Partnerships**:
  + License IP with clearly defined use terms.
* **Education**:
  + Train employees to respect and protect IP.

**4. Security and Privacy Implications of Cloud Computing**

* **What is Cloud Computing?**
  + Using online servers to store, manage, and process data.
* **Security Issues**:
  + **Data Breaches**: Hackers may access cloud-stored data.
  + **Data Loss**: Server failures or accidental deletions.
  + **Insecure Interfaces**: Unsecured APIs can be exploited.
  + **Lack of Control**: Dependence on provider for security.
  + **Data Sovereignty**: Legal issues due to data location.
  + **Shared Resources**: Risk of attacks in multi-tenant environments.

**5. Safe Computing Guidelines**

* **Use Strong Passwords**: Mix of letters, numbers, and symbols.
* **Enable MFA**: Adds an extra verification step.
* **Keep Software Updated**: Avoid vulnerabilities by patching.
* **Avoid Public Wi-Fi for Sensitive Work**: Use VPN if needed.
* **Backup Data Regularly**: Prevent data loss.
* **Avoid Suspicious Attachments**: Could be malware.
* **Lock Devices**: Prevent unauthorized access.
* **Be Cautious with Personal Info**: Share only on secure sites.
* **Report Security Incidents Immediately**: Notify IT or supervisor.
* **Avoid Using Personal Devices for Work**: Use company-approved devices.

**6. Computer Usage Policy**

* **Purpose**: Define how company devices are used responsibly.
* **Authorized Use**: Only for employees and approved tasks.
* **Prohibited Activities**: No illegal or personal use of resources.
* **Software Installation**: Only by authorized personnel.
* **Internet Usage**: Limited to work-related activities.
* **Data Security & Confidentiality**: Follow company protocols.
* **Remote Work Rules**: Secure VPN, encrypted devices.
* **Monitoring & Privacy**: Employees' activity may be monitored.
* **Policy Review**: Updated regularly to reflect changes.