UNIT – 1

Unit: Introduction to Cybercrime

1. Introduction

Cybercrime refers to criminal activities that are conducted through or against computer systems and networks. Unlike traditional crimes, cybercrimes involve the use of technology, especially the Internet, to commit offenses such as data theft, identity fraud, or unauthorized access.

1.1 Definition and Origins of the Word “Cybercrime”

- The term **“Cybercrime”** is derived from the prefix **“cyber”**, which relates to computers, networks, or virtual reality, and **“crime”**, which refers to any act punishable under law.
- In simple terms, **Cybercrime** means **“crime committed using computers and networks”**.
- These crimes often target computers or use them as tools to carry out illegal acts.
- Early examples of cybercrime go back to the 1970s when hackers accessed telephone systems (called *phreaking*) to make free calls.
- The rise of the Internet in the 1990s made cybercrime more widespread — covering financial frauds, hacking, and identity theft.

Formal Definition:

“Cybercrime is any unlawful act where computer, network, or communication devices are used either as a tool or as a target or both.”

1.2 Cybercrime and Information Security

Cybercrime and Information Security are closely related but not the same:

Aspect	**Cybercrime**	**Information Security**
Objective	To commit illegal acts using computers or networks	To protect data and systems from unauthorized access or damage
Focus	Offense	Defense

Aspect	Cybercrime	Information Security
Examples	Hacking, fraud, data theft	Firewalls, encryption, access control

- **Cybercrime** threatens **information security** by violating the **CIA triad** — *Confidentiality, Integrity, and Availability*.
- **Information Security** measures are essential to prevent, detect, and respond to cyber threats.

1.3 Cybercriminals

Cybercriminals are individuals or groups who commit crimes using digital technology.

Categories of Cybercriminals:

1. **Script Kiddies:**
   Inexperienced hackers who use existing tools or scripts developed by others to attack systems.
2. **Crackers:**
   Skilled individuals who break into systems for malicious intent.
3. **Hacktivists:**
   Combine *hacking* with *activism* — attack for political or social causes.
4. **Cyber Terrorists:**
   Attack computer systems to cause fear, panic, or damage critical infrastructure.
5. **Disgruntled Employees:**
   Insiders who misuse access to harm the organization.
6. **Professional Hackers:**
   Experts hired by companies (ethical hackers) or by criminal organizations.

Motives of Cybercriminals:

- Financial gain
- Revenge
- Political agenda
- Challenge or curiosity
- Cyber espionage

Steps followed by cybercriminals for planning an attack.

1. Target selection
   Pick the victim (individual, company, government) based on value, access, or vulnerability.
   Mitigation: Maintain asset inventories and protect high-value assets first.

2. Reconnaissance (Open-source intel & scanning)
   Gather information from public sources (websites, LinkedIn, forums), scan internet-facing systems and enumerate services, emails, and software versions.
   Mitigation: Limit public exposure, use privacy settings, and monitor internet-facing assets.

3. Target profiling & prioritization
   Analyze collected data to identify high-value people/accounts, likely entry points, and useful tools — create a prioritized list of attack vectors.
   Mitigation: Harden accounts of high-risk personnel and enforce least privilege.

4. Threat modeling / attack planning
   Decide the attack method (phishing, malware, supply-chain, insider use) and required resources (malware, fake domains, compromised accounts).
   Mitigation: Threat modeling for defenders—identify likely attack paths and close them.

5. Weaponization
   Build or acquire payloads: phishing templates, malware binaries, exploit scripts, fake websites, or deepfake/audio clips. May use off-the-shelf phishing kits.
   Mitigation: Use threat intelligence to detect such tools and block known payload signatures.

6. Infrastructure setup
   Prepare supporting infrastructure: register look-alike domains, set up C2 (command & control) servers, create fake social accounts, or rent botnets. Ensure anonymity (proxies, VPNs, cryptocurrencies).
   Mitigation: Monitor domain registrations, block suspicious domains, and use DNS filtering.

7. Delivery / initial access
   Send the attack to the target (phishing email, malicious attachment, infected USB, compromised vendor update, SMS link, voicemail).

Mitigation: Email filtering, sandbox attachments, user training, and strict supply-chain controls.

8. Exploitation
   Trigger the vulnerability (user clicks link, opens attachment, or exploit runs) to execute code or capture credentials.
   Mitigation: Patch systems, disable risky macros, and enforce safe browsing and attachment handling.

9. Installation / persistence
   Install backdoors, malware, or create covert accounts to maintain long-term access (scheduled tasks, services, modified registry, web shells).
   Mitigation: Endpoint detection & response (EDR), integrity monitoring, and frequent log reviews.

10. Command & Control (C2) establishment
    Establish a covert channel to communicate with infected hosts (HTTPs callbacks, DNS tunneling, P2P).
    Mitigation: Network monitoring, outbound traffic restrictions, and anomaly detection.

---

2. Classification of Cybercrimes

Cybercrimes can be broadly classified based on the **target** or **means** used.

2.1 Cybercrime Against Individuals

Cybercrimes against individuals are offenses that directly affect a person's privacy, identity, property, or dignity. These crimes exploit computers, mobile devices, or online platforms to target an individual's personal or financial information.
Such crimes may lead to emotional distress, financial loss, or reputational harm.

(a) E-Mail Spoofing

Definition

E-mail spoofing is when someone fakes the sender's address to trick you into thinking an email is from someone you trust..

Explanation

Attackers manipulate the "From" field in an email header so that the message appears legitimate — for example, showing it came from a bank, a government agency, or a friend. These emails often contain malicious attachments or links to fake websites designed to steal passwords or financial details.

Example

A spoofed email may appear as:
From: support@hdfcbank.com
Subject: "Urgent: Verify your account immediately."
When the victim clicks the link, it redirects to a phishing site that captures their login credentials.

Safeguards

- Check the sender's email address carefully.
- Never click on suspicious links or download unknown attachments.
- Enable email authentication technologies like SPF, DKIM, and DMARC.
- Use spam filters and update antivirus software regularly.
- Verify directly with the organization if the email asks for sensitive data.

(b) Spamming

Definition

Spamming refers to sending unsolicited bulk emails to multiple recipients, usually for advertising, phishing, or spreading malware.

Explanation

Spam consumes bandwidth, clogs inboxes, and often contains links to malicious websites that infect systems or steal data.

Example

You receive an email saying, *"You've won a lottery worth ₹10,00,000! Click here to claim."* When clicked, it installs malware or demands personal information.

Safeguards

- Avoid responding to spam messages.
- Use anti-spam filters provided by email services.

- Never share your email address on public forums.
- Use a secondary email for registrations or subscriptions.
- Report spam as “junk” to train filters.

(c) Internet Time Theft

Definition

Internet Time Theft occurs when a person illegally uses another person’s Internet account without authorization.

Explanation

This was common during the dial-up era, where attackers used stolen credentials to connect to the Internet at someone else’s expense.
Today, it may occur via Wi-Fi theft or misuse of shared hotspots.

Example

A hacker gains access to your Wi-Fi network and downloads large files, causing your Internet bill to rise.

Safeguards

- Set strong Wi-Fi passwords using WPA3 encryption.
- Regularly check the list of connected devices.
- Avoid sharing Internet credentials publicly.
- Enable network monitoring tools.

(d) Industrial Spying / Espionage

Definition

Industrial Espionage is the act of stealing confidential business information, trade secrets, or research data using illegal means, often through hacking.

Explanation

Competitors or insider employees may install spyware or use phishing to gather business intelligence.

Example

A rival company hacks into another’s server to steal product design or pricing strategy.

Safeguards

- Implement data encryption and access control policies.
- Conduct employee awareness training.
- Use Intrusion Detection Systems (IDS) and firewalls.
- Sign Non-Disclosure Agreements (NDAs) with employees and contractors.

(e) Hacking

Definition

Hacking is unauthorized access to computer systems or networks with the intention to steal, alter, or destroy data.

Types of Hackers

- White Hat Hackers: Ethical hackers who test security systems.
- Black Hat Hackers: Malicious hackers who exploit systems.
- Grey Hat Hackers: Hackers who expose vulnerabilities without permission.

Example

An attacker breaks into a company's database and steals customer credit card information.

Safeguards

- Keep systems updated and patched.
- Use strong passwords and multi-factor authentication.
- Install firewalls and antivirus software.
- Perform regular security audits.

(f) Online Frauds

Definition

Online fraud is when criminals use the Internet to trick people. They do this to steal money, personal information, or even pretend to be someone else to gain access to accounts. These scams can happen through fake websites, emails, or messages.

Types

- Phishing: Fake websites resembling legitimate ones to steal credentials.
- Online Auction Fraud: Seller never delivers the purchased product.
- Investment Scams: Fake schemes promising quick profits.
- Job Frauds: Asking candidates to pay for fake job offers.

Example

A user applies for a “work-from-home” job and is asked to pay ₹2,000 as registration fees — later, the company disappears.

Safeguards

- Verify the authenticity of websites and job offers.
- Avoid sharing personal or banking information online.
- Use secure (https://) connections.
- Check reviews and legitimacy before online transactions.

(g) Pornographic Offenses

Definition

The publication, transmission, or possession of obscene or sexually explicit content in electronic form is a punishable cyber offense.

Explanation

Includes adult content distribution, child pornography, or the use of digital platforms for exploitation.
Under Section 67 of the IT Act, 2000, publishing or transmitting obscene material in electronic form is illegal.

Example

Uploading explicit images of a person without consent on social media.

Safeguards

- Avoid visiting or sharing adult or obscene content.
- Report such content to cyber police or CERT-IN.
- Use parental controls for minors.

- Always obtain consent before sharing media.

(h) Software Piracy

Definition

Software piracy is the illegal copying, distribution, or use of software without proper licensing.

Forms

- Counterfeiting: Selling fake copies.
- End-User Piracy: Installing software on multiple systems without license.
- Hard-Disk Loading: Vendors pre-installing unlicensed software.
- Internet Piracy: Sharing software on peer-to-peer networks.

Example

Downloading paid software like Microsoft Office from torrent sites without license.

Safeguards

- Use genuine software and verify licenses.
- Enable automatic updates from official sources.
- Educate users about copyright laws.
- Use Digital Rights Management (DRM) tools.

(i) E-Mail Bombing

Definition

E-mail bombing is a denial-of-service attack where a large number of emails are sent to a victim’s inbox to crash or block it.

Example

Sending thousands of emails per second to an organization’s server, causing it to slow down or crash.

Safeguards

- Use email filters and anti-spam controls.
- Configure rate-limiting on mail servers.
- Report abuse to the email service provider.
- Employ firewalls to detect abnormal traffic.

(j) Password Sniffing

Definition

Password sniffing is the process of intercepting and capturing passwords transmitted over a network.

Explanation

Hackers use tools known as packet sniffers to read network data packets and extract login details, especially on unsecured networks.

Example

Using Wi-Fi in a public café without encryption — hackers can capture your login credentials.

Safeguards

- Avoid logging in on public Wi-Fi.
- Use VPN (Virtual Private Network) for encrypted connections.
- Prefer HTTPS websites.
- Change passwords regularly and use password managers.

(k) Credit Card Frauds

Definition

Credit card fraud involves unauthorized use of credit or debit card information to make fraudulent purchases.

Methods

- Phishing Emails – Asking for card details.
- Skimming Devices – Installed on ATMs or POS machines.
- Fake E-commerce Sites – Imitating genuine platforms.
- Data Breaches – Hackers steal stored card data.

Example

A fake shopping website collects card details and misuses them for unauthorized transactions.

Safeguards

- Shop only from trusted and secure (https) sites.
- Enable SMS/Email alerts for transactions.
- Avoid saving card details on websites.
- Report lost or stolen cards immediately.
- Use virtual cards or OTP-based verification.

Conclusion

Cybercrimes against individuals continue to grow as technology advances. Awareness, strong security practices, and responsible digital behavior are essential to safeguard oneself. Every Internet user should stay informed about potential threats and follow cybersecurity hygiene to prevent being a victim.

Summary

Category	**Example Crimes**
Against Individuals	Hacking, Identity Theft, Cyberstalking
Against Organizations	Data theft, Espionage, DoS attacks
Against Government	Cyber Terrorism, Espionage
Against Society	Child pornography, Hate speech

---

4. Legal Framework (from Nina Godbole – Reference)

- **IT Act, 2000** (Amended in 2008) is India's main law governing cybercrimes.
- Defines cyber offenses like:
  - Unauthorized access (Sec. 43)
  - Identity theft (Sec. 66C)
  - Cheating by impersonation using computer resources (Sec. 66D)
  - Publishing obscene material (Sec. 67)
  - Cyber terrorism (Sec. 66F)

A. Common techniques used to launch phishing attacks

1. Email spoofing / forged headers
   - What: Forge the "From" address and email headers so a message appears from a trusted sender (bank, coworker, vendor).
   - Why it works: People trust the displayed sender.
   - Indicator: Sender name looks right but the actual address is odd (e.g., support@paypa1.com).
   - Mitigation: SPF/DKIM/DMARC email authentication; filter and quarantine suspicious mail.
2. Malicious links (URL masking / redirection / typosquatting / homograph attacks)
   - What: Send links that look legitimate but go to malicious pages (using similar-looking domains, tiny typos, percent-encoding, or punycode homographs).
   - Why it works: Users click without inspecting the real URL.
   - Indicator: URL doesn't match the displayed link; contains odd characters or long redirect chains.
   - Mitigation: Hover to preview URLs, use browser phishing filters, use DNS filtering and blocklists.
3. Fake login pages / credential harvesting

- What: Create a cloned website that captures usernames/passwords when submitted.
- Why it works: Users enter credentials believing the site is genuine.
- Indicator: Slightly different page design, no HTTPS lock (or mismatched cert), unexpected prompts for credentials.
- Mitigation: Use MFA, check certificate details, use password managers (they won't autofill on wrong domains).

4. Malicious attachments and weaponized files
    - What: Attach Office docs, PDFs, archives or executables that contain macros, scripts, or exploits to drop malware.
    - Why it works: Users open attachments that look business-related.
    - Indicator: Unexpected attachments, macro prompts, double extensions (invoice.pdf.exe).
    - Mitigation: Block risky attachment types, sandbox attachments, disable macros by default, endpoint protection.
5. Social engineering (urgency/fear/trust manipulation)
    - What: Messages that create panic (account locked, urgent invoice), or exploit trust (CEO need, HR request).
    - Why it works: Emotional reaction makes users skip verification.
    - Indicator: Urgent language, requests for immediate action, private info requests.
    - Mitigation: User awareness training, verification procedures (call-back policy), slow-down prompts.
6. Spear-phishing preparatory reconnaissance
    - What: Harvest info (LinkedIn, social media, company site) to craft targeted, convincing messages.
    - Why it works: Personalized content increases credibility.
    - Indicator: Highly specific references to projects, colleagues, or schedules.

- Mitigation: Limit public exposure of sensitive info, privacy settings, employee training.

7. Business Email Compromise (BEC) / CEO fraud techniques
    - What: Compromise or impersonate executives/suppliers to request wire transfers or sensitive changes. May use account takeover or lookalike addresses.
    - Why it works: High trust and authority make requests compliant.
    - Indicator: Unusual payment instructions, out-of-process requests, sender domain variations.
    - Mitigation: Dual-approval payment controls, verify changes by voice/video call, email anomaly detection.

8. Smishing & Vishing (SMS and voice phishing)
    - What: SMS links or voice calls that request verification codes, personal info, or trick victims into installing apps.
    - Why it works: Mobile users act quickly; caller ID can be spoofed.
    - Indicator: Unsolicited SMS with links, recorded urgent voicemail asking for OTP.
    - Mitigation: Don't share OTPs, verify callers via known numbers, use carrier spam filters.

9. Pharming / DNS poisoning / redirect attacks
    - What: Corrupt DNS records or hosts files so a legitimate domain resolves to an attacker site.
    - Why it works: Users type a trusted domain but are routed to malicious server.
    - Indicator: Certificate warnings, unexpected site behavior.
    - Mitigation: DNSSEC, secure DNS resolvers, monitor DNS records and changes.

10. Watering-hole attacks
    - What: Compromise websites frequented by a target group to deliver exploits or phishing to visitors.

- Why it works: Trust in commonly used sites lowers suspicion.
- Indicator: Popular site behaving strangely, or sudden redirects.
- Mitigation: Browser security updates, network monitoring, use content security policies.

B. Types of phishing attacks

1.Bulk / Mass Phishing

- Def: Non-targeted emails sent to thousands.
- Example: "You've won a prize — click to claim."
- Targets: General public.

2. Spear Phishing
    - Def: Highly targeted phishing tailored to a specific person or role using personal info.
    - Example: Email referencing a recent meeting and request for attached invoice.
    - Targets: Specific individual(s).
3. Whaling
    - Def: Spear phishing targeted at high-value executives (CEOs, CFOs).
    - Example: Fake legal subpoena or urgent wire transfer request from "CEO."
    - Targets: Executives and decision-makers.
4. Clone Phishing
    - Def: Attacker creates a nearly identical copy of a previously legitimate email but replaces links/attachments with malicious ones.
    - Example: A resend of a real invoice with a malicious link replacing the genuine one.
5. Business Email Compromise (BEC) / CEO Fraud

- Def: Impersonation of executives or suppliers to authorize fraudulent transfers or data disclosure.
- Example: “Finance, send immediate $50,000 to this vendor account.”
- Targets: Finance departments, HR.

6. Pharming
    - Def: Redirect users from legitimate sites to malicious ones by poisoning DNS or changing host files.
    - Example: Bank URL resolves to attacker server that looks identical to bank’s site.
7. Smishing (SMS phishing)
    - Def: Phishing via SMS messages containing malicious links or instructions.
    - Example: ”Your bank blocked a transaction. Confirm here: .”
8. Vishing (voice phishing)
    - Def: Phishing via telephone calls or voice messages that manipulate victims to reveal info or transfer money.
    - Example: Caller poses as bank support asking for OTP.
9. Angler Phishing / Social Media Phishing
    - Def: Using social platforms to impersonate support accounts or lure users to malicious pages.
    - Example: Fake Twitter support DM with link requesting login.
10. Man-in-the-Middle Phishing
    - Def: Intercept credentials or modify content between user and service (often via rogue Wi-Fi).
    - Example: Captive portal that asks for social media credentials and sends them to attacker.
11. Credential Stuffing (related technique)

    - Def: Using leaked username/password pairs from breaches to try logins on other sites; often combined with phishing to obtain initial credentials.
    - Example: Using breached password to access a user’s bank on another site.

12. Watering-hole phishing
    - Def: Compromise a site popular among target group to serve malware or phishing content.
    - Example: A trade-association site hacked to deliver fake updates with malicious links.
13. Deepfake / Synthetic Phishing
    - Def: Use of AI-generated voice or video to impersonate leadership for fraud.
    - Example: Audio of a manager instructing finance to release funds.

Quick detection checklist (for users)

- Check sender email address carefully (not just display name).
- Hover over links to inspect real URL before clicking.
- Look for generic greetings, poor grammar, and urgent tone.
- Verify requests for money or data via a second channel (call the known number).
- Don’t open unexpected attachments; scan them in a sandbox.
- Be suspicious of requests for OTPs or confirmation codes.

Best mitigations & enterprise controls

- MFA / 2FA (very effective against credential theft).
- Email authentication: SPF, DKIM, DMARC and DMARC reporting.
- Secure email gateways & anti-phishing filters.
- URL and DNS filtering, blocklists, and safe-browsing services.

- Endpoint protection (EDR) and attachment sandboxing.
- Security awareness training & simulated phishing to change user behavior.
- Least privilege & transaction controls (dual approvals for wire transfers).
- Threat intelligence & domain monitoring to detect lookalikes and phishing kits.
- Incident response playbooks for suspected compromises and BEC events.