INTRODUCTION TO CYBER CRIME

*Quick Exam Notes for Unit (**1**)*
*Brought to you by **ZenYukti***

1. Cybercrime — Definition & Origins

- **Cybercrime:** Any criminal activity involving a computer, network, or digital device
- Also called: Computer Crime, e-Crime, Hi-Tech Crime, Electronic Crime
- Term 'Cybercrime' comes from 'Cyberspace' — coined by William Gibson in novel Neuromancer (1984)
- Cyberspace = virtual world of interconnected computers and networks

- **Information Security (InfoSec):** Protecting information from unauthorized access, use, disclosure, disruption, modification or destruction
- Three pillars of InfoSec — CIA Triad:
  - **Confidentiality — only authorized access**
  - **Integrity — data is accurate and unaltered**
  - **Availability — systems accessible when needed**

2. Who Are Cybercriminals?

- Not just 'hackers in hoodies' — wide range of individuals

Type	Description
Hackers	Break into systems; may be ethical (white hat) or malicious (black hat)
Crackers	Break software protections, defeat copy protection
Script Kiddies	Unskilled attackers using pre-written scripts/tools
Insiders	Employees/ex-employees misusing access
Phreakers	Manipulate telephone/telecom systems
State-Sponsored	Government-backed attackers for espionage/sabotage
Cyber Terrorists	Use cyberspace to create terror, disrupt critical infrastructure
Hacktivists	Hack for ideological/political reasons (e.g. Anonymous)

3. Classification of Cybercrimes

A) Against Individuals

- Cyberstalking, Harassment, Identity theft, Phishing, Email spoofing
- Child pornography, Cyber defamation, Impersonation

B) Against Property

- Hacking, Computer vandalism, Transmitting viruses, IPR violations
- Cybersquatting (domain name theft), Cyber extortion

C) Against Organizations

- Unauthorized access, DoS/DDoS attacks, Virus/malware attacks
- Email bombing, Salami attacks (small unnoticed thefts), Logic bombs

D) Against Society / Government

- Cyber terrorism, Cyber warfare, Trafficking, Financial crimes
- Forgery, Pornography distribution

4. A Global Perspective on Cybercrimes

- Cybercrime is BORDERLESS — attackers and victims can be in different countries
- Major global threats: Identity theft, financial fraud, data breaches, ransomware
- Difficult to prosecute — different countries have different laws
- **USA:** Computer Fraud and Abuse Act (CFAA), FBI Cyber Division
- **India:** IT Act 2000 (amended 2008), Cyber Cells in police departments
- **Global bodies:** INTERPOL Cybercrime Unit, EC3 (Europol), CERT teams
- G8 countries coordinate on cybercrime through 24/7 network
- Budapest Convention (2001) — first international treaty on cybercrime

⚠ *Jurisdiction is the biggest challenge in global cybercrime prosecution*

5. Cybercrime Era — Survival Mantra for Netizens

- Netizen = citizen of the internet — anyone who uses the web
- Key survival tips:
  - **Use strong, unique passwords + enable 2FA**
  - **Keep software/OS updated (patches fix vulnerabilities)**
  - **Don't click unknown links — phishing awareness**
  - **Use HTTPS sites; avoid public Wi-Fi for sensitive tasks**
  - **Regular data backups (protect against ransomware)**
  - **Install reputable antivirus/firewall**
  - **Don't overshare personal info on social media**
  - **Verify before trusting emails, calls, messages (social engineering awareness)**
  - **Check app permissions; don't grant unnecessary access**

⚠ *Most attacks succeed because of human error, not technical failure*

6. Cyber Offenses — How Criminals Plan Attacks

- Attackers follow a systematic process:

Phase	What Happens
1. Reconnaissance	Gather info about target — passive (OSINT) or active (probing)
2. Scanning	Find open ports, vulnerabilities, live systems (nmap, etc.)
3. Gaining Access	Exploit vulnerabilities — via malware, phishing, brute force
4. Maintaining Access	Install backdoors, rootkits to retain control
5. Covering Tracks	Delete logs, hide evidence to avoid detection

- **OSINT:** Open Source Intelligence — gathering info from public sources (social media, websites, public records)
- **Footprinting:** Collecting info about a target before attacking (part of recon)

7. Social Engineering

- **Definition:** Manipulating PEOPLE (not systems) into revealing confidential info or performing actions
- Exploits human psychology — trust, fear, urgency, authority
- Most dangerous attack vector — no technical skill needed

Technique	How It Works
Phishing	Fake emails/sites trick users into entering credentials
Vishing	Voice calls (phone) pretending to be bank/IT/police
Smishing	SMS-based phishing — fake text messages with links
Pretexting	Attacker creates a fabricated scenario to extract info
Baiting	Leaving infected USB drives hoping victims plug them in

Quid Pro Quo	Offer help (fake IT support) in exchange for access/info
Tailgating/Piggybacking	Physically following someone into a restricted area
Spear Phishing	Targeted phishing — customized for a specific individual
Whaling	Spear phishing aimed at high-level executives (CEO, CFO)

⚠ *Defence: Awareness training, verify before trusting, never share passwords over phone/email*

8. Cyberstalking

- **Definition:** Using internet/technology to stalk, harass, or threaten a person repeatedly
- Methods used:
  - **Sending threatening/abusive emails repeatedly**
  - **Tracking location via GPS, social media check-ins**
  - **Posting defamatory content about victim online**
  - **Monitoring victim's online activity**
  - **Identity theft to destroy reputation**
- Victims: often women, children, ex-partners
- **India:** Punishable under IT Act 2000 + Section 354D IPC (stalking)
- **Difference from physical stalking:** Cyberstalking crosses geographic boundaries instantly

⚠ *Report to Cyber Cell immediately; save all evidence (screenshots, emails)*

9. Cybercafe and Cybercrimes

- Cybercafes are high-risk environments for cybercrime:
  - **Shared computers — keyloggers may be installed**
  - **Unsecured networks — easy to sniff traffic**
  - **No accountability — hard to trace anonymous users**
  - **Criminals use them to avoid being traced**
- Common crimes at cybercafes:
  - **Email hacking, online fraud, viewing/distributing illegal content**
  - **Identity theft using saved passwords**
- India's IT Act requires cybercafe owners to maintain user logs
- Guidelines: Cybercafe owners must register users, maintain visit records

⚠ *Never log into banking or personal accounts from a cybercafe*

10. Botnets — The Fuel for Cybercrime

- **Bot:** Compromised computer running malicious software controlled remotely
- **Botnet:** Network of thousands/millions of infected bots controlled by one attacker (Bot Herder)
- **Bot Herder / Bot Master:** The attacker who controls the botnet
- **C&C Server:** Command and Control server — used to send instructions to bots

- How a Botnet is Created:
  - **Malware spread via phishing emails, drive-by downloads, infected USB**
  - **Victims' machines get infected (become 'zombies')**
  - **Zombies connect back to C&C and await commands**

- Uses of Botnets:

Attack Type	Description
DDoS Attacks	Flood a target with traffic from thousands of bots, crashing it
Spam Campaigns	Send millions of spam/phishing emails
Click Fraud	Bots click ads to generate fake revenue
Credential Stuffing	Test stolen username/password combos across many sites

Cryptomining	Use victims' CPU to mine cryptocurrency without their knowledge
Data Theft	Steal sensitive data from infected machines

⚠ *Defence: Keep OS patched, use firewall, monitor unusual outbound traffic*

11. Attack Vector

- **Attack Vector:** The pathway or method used by an attacker to gain unauthorized access to a system
- Common Attack Vectors:

Attack Vector	Description
Phishing / Email	Malicious links/attachments sent via email
Malware	Viruses, Trojans, Ransomware, Spyware, Worms
Man-in-the-Middle (MitM)	Attacker intercepts communication between two parties
SQL Injection	Malicious SQL code inserted into input fields to access DB
Cross-Site Scripting (XSS)	Inject malicious scripts into web pages viewed by others
Brute Force	Try all possible passwords until correct one found
Zero-Day Exploit	Exploit an unknown/unpatched vulnerability
Drive-by Download	Malware downloaded just by visiting a malicious website
Insider Threat	Employees misuse legitimate access
Physical Access	Attacker physically accesses device (USB drop, hardware keylogger)
Weak Passwords	Easily guessable or reused passwords compromised
Unpatched Software	Exploiting known vulnerabilities in outdated software

- **Attack Surface:** Total set of points where an attacker can try to enter a system — reduce it to improve security

⚠ *Patch regularly + least privilege principle = reduce attack surface significantly*

12. QUICK RECAP TABLE

Topic	Key Point to Remember
Cybercrime origin	From 'Cyberspace' — coined by William Gibson (1984)
CIA Triad	Confidentiality, Integrity, Availability
Script Kiddie	Unskilled hacker using pre-written tools
Social Engineering	Manipulate people, not systems — exploits human psychology
Phishing	Fake emails/sites to steal credentials
Whaling	Phishing targeting high-level executives
Cyberstalking	Online harassment using repeated digital contact
Botnet	Network of infected zombie computers (C&C controlled)
Bot Herder	The attacker controlling the botnet
DDoS	Distributed Denial of Service — flood target using botnet
Attack Vector	Method used to access a system illegally
Zero-Day	Exploit for unknown/unpatched vulnerability
Budapest Convention	First international cybercrime treaty (2001)
India's Law	IT Act 2000, amended 2008

END OF NOTES

ZenYukti

Quick Exam Notes

zenyukti.in

Other Unit Notes

All subject notes on GitHub — free to access & star

github.com/ZenYukti/MyNotes

Join ZenYukti Discord

Free workspace — internship & hackathon updates, tech discussions

go.zenyukti.in/discord

FIND US ON

Made with care by **ZenYukti** · Share freely, learn together

Quick Exam Notes | Exam Ready | Free Resource