AKTU

GATEWAY CLASSES

B.Tech 2nd Year

All Branches

ONE SHOT

Cyber Security

Unit-1 Introduction To Cyber Crime

Download Free Notes from App

CYBER SECURITY

Syllabus Unit-1

INTRODUCTION TO CYBER CRIME : Cybercrime- Definition and Origins of the word Cybercrime and Information Security, Who are Cybercriminals? Classifications of Cybercrimes, A Global Perspective on Cybercrimes, Cybercrime Era: Survival Mantra for the Netizens.

Cyber offenses: How Criminals Plan the Attacks, Social Engineering, Cyber stalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector.

Cyber Security

Definition : Cyber Security is the practice of protecting systems , networks and program from digital attacks.

“Cyber security is the protection of internet-connected systems, including hardware, software and data, from cyber attacks”.These cyberattacks are usually aimed at accessing ,changing or destroying sensitive information .

Need of Cyber Security

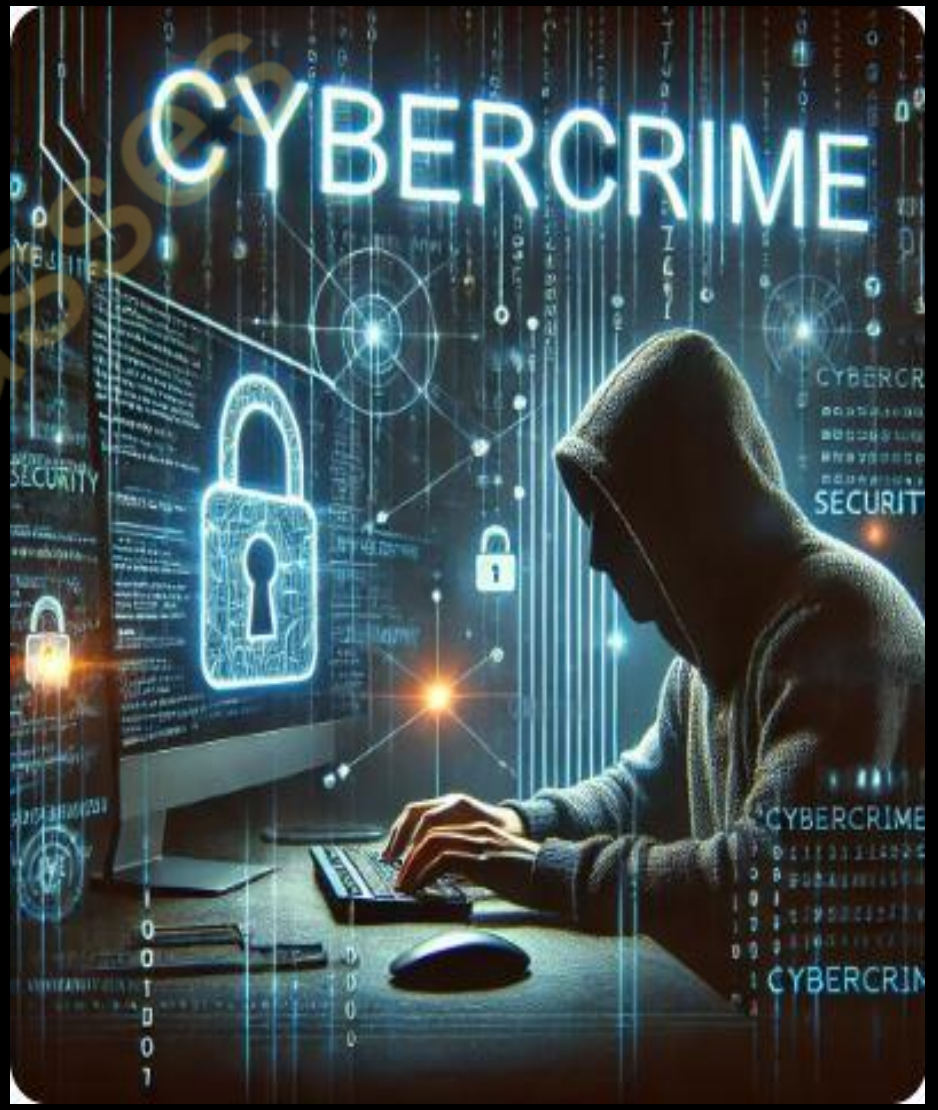
- To protect our private data
- To protect intellectual data
- To protect banking and financial data
- National Security
- To protect our sensitive data

Cybercrime

- Cybercrime is a “unlawful acts wherein the computer is either a tool or target or both”.

Alternative Definitions of Cybercrime

- Cybercrime involves any criminal activity conducted using digital technology.
- Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.
- Cybercrime is illegal activity involving computers, the internet, or network devices.
- Any financial dishonesty that takes place in a computer environment.
- The term “cybercrime” relates to a numbers of other terms i.e., Computer-related crime, Computer crime, Internet crime, E-crime, High-tech crime, etc.



Types of attack prevalent in Cybercrime

Some people argue that a cybercrime is not a crime as it is a crime against software & not against a person (or) property. However, while the legal systems around the world scramble to introduce laws to combat cyber criminals.

Two types of attacks prevalent in cybercrime:

1. Techno-crime: The primary goal of techno-crime is typically financial gain, theft of information, or causing harm to individuals, organizations, or society . It is premeditated act against a system or systems, with the intent to copy, steal, prevent access, corrupt or otherwise deface or damage parts of or the complete computer system .Example : Imagine someone hacks into a bank's computer system and steals money from people's accounts.

2. Techno-vandalism: Techno-vandalism is when someone uses technology to intentionally cause damage or disrupt systems, but not necessarily for financial gain. Example: If someone spreads a computer virus that crashes other people's computers or websites just for fun or to cause trouble, that's techno-vandalism. They're not trying to steal anything, just to cause harm or disruption.

Difference b/w Cybercrime and Traditional Crime

Aspect	Cybercrime	Traditional Crime
Definition	Crimes committed using computers and the internet.	Crimes committed without the use of digital technology.
Tools Used	Computers, smartphones, networks, and other digital devices.	Physical tools like weapons
Location	From any location with internet access.	Typically localized and requires physical presence.
Evidence Collection	Digital evidence like logs, IP addresses, and digital footprints.	Physical evidence like fingerprints, DNA, and physical artifacts.
Examples	Hacking a company's database to steal sensitive information.	Breaking into a house to steal valuables.

Classification Of Cyber Crime

- **Cybercrime Against Individual:** Cybercrime against individuals refers to criminal activities conducted using digital technologies that specifically target personal information, reputation, and personal safety of individuals.
- **Cybercrime Against Property:** Cybercrime against property refers to illegal activities conducted via digital means that target an individual's or organization's property, including financial assets, intellectual property, and data.
- **Cybercrime Against Organization :** Cybercrime against organizations involves illegal activities that target a company's digital assets, systems, and data, often leading to financial loss, reputational damage, and operational disruptions.
- **Cybercrime Against Society:** Cybercrime against society refers to illegal activities conducted through digital means that impact the broader public or specific groups within society. For Example :Banned websites illegal materials are made available to the people through the internet.

CLASSIFICATION OF CYBER CRIME

Cybercrime Against Individual

1. E-Mail Spoofing: A spoofed E-Mail is one that appears to originate from one source but has been sent from another source.
2. Spamming: People who create electronic Spam are called spammers. Spam is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unrequested bulk messages.
3. Cyber Defamation: It occurs when defamation takes place with the help of computers and/or the Internet. For example, someone publishes defamatory matter about someone on a website or sends an E-Mail containing defamatory information to all friends of that person.
4. Cyber stalking: Cyberstalking involves the use of the internet and other electronic means to repeatedly harass, intimidate, or threaten an individual, causing fear and distress. It includes behaviors such as sending threatening messages, monitoring online activities, and spreading false information.

Cybercrime Against Property

1. Credit Card Frauds: Credit card fraud is an inclusive term for fraud committed using a payment card, such as a credit card or debit card. The purpose may be to obtain goods or services, or to make payment to another account which is controlled by a criminal.

2. Intellectual Property (IP) Crimes: Cyber theft of IP means stealing of copyrights, software piracy, trade secrets, patents etc., using internet and computers.

3.Internet time theft: Such a theft occurs when an unauthorized person uses the Internet hours paid for by another person.

Cybercrime Against Organization

1. E-Mail bombing/Mail bombs: E-Mail bombing refers to sending a large number of E-Mails to the victim to crash victim's E-Mail account (in the case of an individual) or to make victim's mail servers crash .

2. Salami Attack/Salami technique: These attacks are used for committing financial crimes. The idea here is to make the alteration so insignificant that in a single case it would go completely unnoticed; For example a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 2/- or a few cents in a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount every month.

3. Logic Bomb: A Logic Bomb is a piece of often-malicious code that is intentionally inserted into software. It is activated upon the host network only when certain conditions are met.

4. Trojan Horse : Trojan Horse is a term used to describe malware that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system.

5. Data Diddling: A data diddling (data cheating) attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

Cybercrime Against Society

1. Forgery: Currency notes, postage and revenue stamps, marksheets, etc. can be forged using sophisticated computers, printers and scanners.
2. Cyberterrorism: It is defined as “any person, group or organization who, with terrorist intent, utilizes accesses or aids in accessing a computer or computer network.
3. Web Jacking: Web jacking occurs when someone forcefully takes control of a website (by cracking the password and later changing it). Thus, the first stage of this crime involves “password sniffing”. The actual owner of the website does not have any more control over what appears on that website

Origin Of The Word ”Cybercrime

The term "cybercrime" originates from the combination of "cyber," which pertains to cybernetics and technology, particularly computer networks, and "crime," referring to illegal activities. Here's a brief history of its :

- Cybernetics: The word "cyber" is derived from "cybernetics," a term coined in 1948 by Norbert Wiener. Cybernetics itself comes from the Greek word "Kubernetes," meaning "steersman" or "governor." It pertains to the science of control and communication in animals, humans, and machines. The term "cyber" started to be used more broadly in the context of computers and networks by the 1980s , popularized by science fiction literature, William Gibson's work. The prefix "cyber-" began to appear in various compound words related to computer technology and virtual reality.

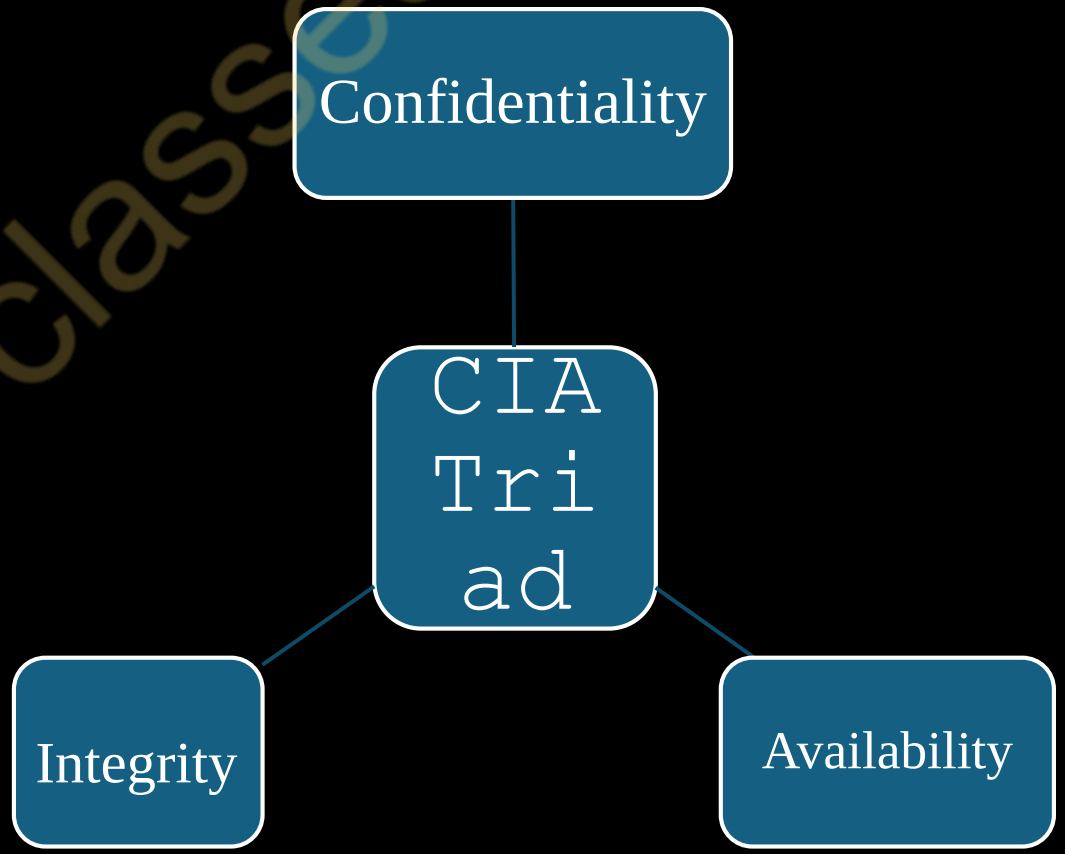
- Crime: The word "crime" has ancient roots, originating from the Latin "crimen," meaning "accusation" or "charge." The term "cybercrime" started to be used in the late 20th century as digital technology advanced, encompassing illegal activities conducted through computer networks, such as hacking, online fraud, and identity theft.

Information Security

Information security (InfoSec) refers to the processes and methodologies involved in protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. It encompasses a wide range of practices and principles aimed at safeguarding data integrity, confidentiality, and availability.

The CIA Triad is a fundamental concept in information security that stands for:

1. **Confidentiality**: Ensuring that information is accessible only to those authorized to have access. Techniques to maintain confidentiality include encryption, access controls, and authentication mechanisms.



2. Integrity: Ensuring the accuracy and completeness of information and processing methods. Measures to maintain integrity include checksums, hashing, and digital signatures, which help in detecting unauthorized alterations to data.

3. Availability: Ensuring that authorized users have access to information and associated assets when required. Strategies to ensure availability include implementing redundant systems, regular maintenance, and protection against denial-of-service (DoS) attacks.

The CIA Triad		
What Is the CIA?		
Confidentiality	**Integrity**	**Availability**
The information is safe from accidental or intentional disclosure.	The information is safe from accidental or intentional modification or alteration.	The information is available to authorized users when needed.
Example		
I send you a message, and no one else knows what that message is.	I send you a message, and you receive exactly what I sent you (without any modification)	I send you a message, and you are able to receive it.
What's The Purpose of the CIA?		
Data is not disclosed	Data is not tampered	Data is available
How Can You Achieve the CIA?		
e.g., Encryption	e.g., Hashing, Digital signatures	e.g., Backups, redundant systems
Opposite of CIA		
Disclosure	Alteration	Destruction

Types of Information Security

1. Network Security: Protects the usability and integrity of network and data. This includes protecting the network from attacks such as distributed denial-of-service (DDoS) attacks and unauthorized access.

2. Application Security: Focuses on keeping software and devices free of threats. Security measures include code reviews, secure coding practices, and application firewalls.

3. Endpoint Security: Involves securing end-user devices such as computers, mobile devices, and tablets. This can include antivirus software, intrusion detection systems, and endpoint detection and response.

4. Data Security: Protects data in storage and in transit. Methods include encryption, masking, and tokenization to ensure data confidentiality and integrity.

5. Identity and Access Management (IAM): Ensures that only authorized users have access to resources. This includes policies, processes, and technologies used to manage digital identities and control access to resources.

6.Cloud Security: Involves securing data, applications, and services hosted in the cloud. This includes ensuring compliance with regulatory requirements and protecting against data breaches and loss.

7.Information Security Governance: Encompasses the policies, procedures, and practices that ensure the effective and efficient use of information security within an organization. This includes risk management, compliance, and incident response planning.

8.Cryptography: The practice of securing information by transforming it into an unreadable format, only accessible by those possessing the decryption key. This ensures confidentiality and integrity of data.

9.Physical Security: Protects physical hardware and infrastructure from physical threats such as theft, vandalism, natural disasters, and unauthorized access.

10. Incident Response: The approach taken by an organization to prepare for, detect, contain, and recover from an information security incident. This includes having an incident response plan and team in place.

Cybercriminals

Cyber criminals are individuals or groups who use computers and the internet to commit crimes. They use digital tools and systems to exploit weaknesses in the system to steal personal information, money, or sensitive data, or to disrupt services. Cyber criminals often aim to make a profit, but some may also be motivated by personal grudges, political reasons, or the challenge of breaking into secure systems. They can operate alone or as part of organized groups, and their actions can impact individuals, businesses, and governments. Examples of their activities include hacking into systems, spreading viruses, committing online fraud, and launching cyberattacks.

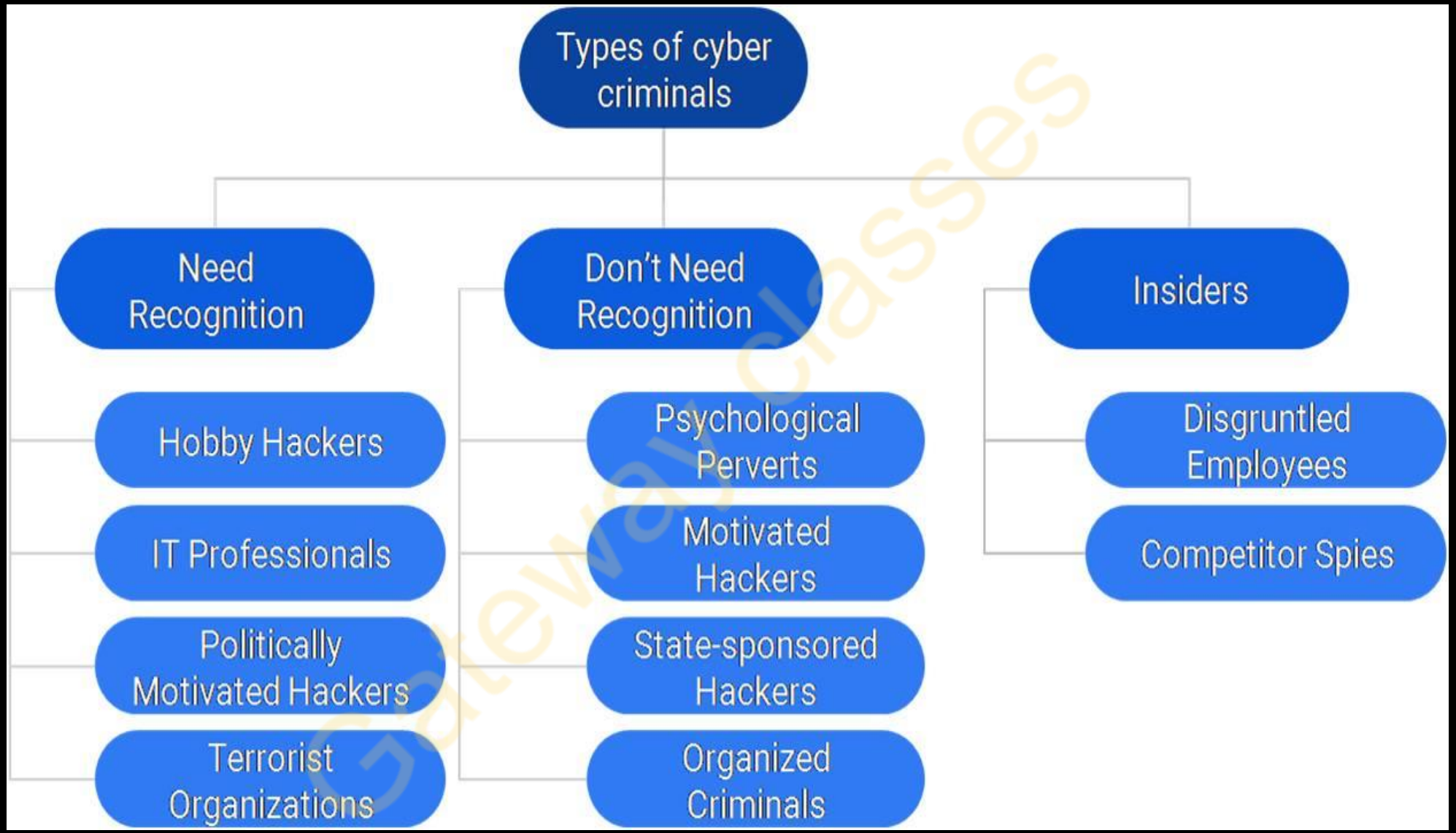
Types of Cybercriminals

Cybercriminals can be divided into three categories as given below:

1.Cybercriminals who are hungry for recognition

2.Cybercriminals who are not interested in recognition

3.Cybercriminals who are insiders


Types of cyber criminals
Need Recognition
Don't Need Recognition
Insiders
Hobby Hackers
IT Professionals
Politically Motivated Hackers
Terrorist Organizations
Psychological Perverts
Motivated Hackers
State-sponsored Hackers
Organized Criminals
Disgruntled Employees
Competitor Spies

1. Cybercriminals who are hungry for recognition

- **Hobby Hackers:** These hackers engage in hacking for fun and intellectual challenge. They enjoy exploring systems and learning about cybersecurity, often without malicious intent.
- **IT Professionals:** Skilled individuals who might hack to demonstrate their abilities, gain recognition in the tech community, or improve their job prospects. They can sometimes blur ethical lines if they hack without permission.
- **Politically Motivated Hackers:** Also known as hacktivists, these hackers conduct attacks to promote political or social causes. They seek to draw attention to their message through their actions.
- **Terrorist Organizations:** Groups that use hacking to further their extremist agendas. They seek recognition to spread fear, disrupt systems, and promote their ideologies.

2. Cybercriminals who are not interested in recognition

- **Psychological Perverts:** Cybercriminals who engage in deviant activities for personal gratification. This can include cyberstalking, online harassment, and other forms of digital abuse.
- **Motivated Hackers:** These hackers are primarily driven by financial gain. They aim to steal money or valuable data while avoiding detection. Examples include identity thieves and financial loss.
- **State-Sponsored Hackers:** Hackers working for government entities to conduct cyber warfare. Their actions are secretive and aim to serve national interests.
- **Organized Criminals:** Groups that engage in hacking as part of broader criminal operations. They may run large-scale scams, ransomware attacks, or other illegal activities for profit.

3. Cybercriminals who are insiders

- **Disgruntled/Dissatisfied Employees:** Current or former employees who feel wronged by their employer and seek revenge. They may steal data or leak sensitive information.

- **Competitor Spies:** Competitor Spies refers to individuals or groups who secretly gather information from within a company to help a competitor or to further their own criminal activities. They might be hired by rival businesses.

A Global Perspective On Cybercrime

Cybercrime is a growing global threat, impacting individuals, businesses, and governments across the world. A global perspective on cybercrime involves understanding the scope, impact and challenges of cybercriminals activity across the international borders. Here's the global perspective on the issue:

- Growing Threat: Cybercrime is increasing worldwide as more people and devices connect to the internet.
- Economic Impact: It costs the global economy billions of dollars annually, including direct theft, recovery costs, and lost trust.
- Privacy Concerns: Data breaches expose personal information, leading to identity theft and privacy violations.
- Global Reach: Cybercriminals can target anyone, anywhere, making it a worldwide issue .
- Organized Crime: Many cybercriminals operate in organized groups, sometimes with state support, and use the dark web for illegal activities.
- Regulation and Cooperation: Countries are creating laws to fight cybercrime, but effectiveness varies. International cooperation is crucial.
- Challenges: Identifying attackers is difficult due to internet anonymity, and threats evolve quickly, making defense challenging.
- Future Trends: Technologies like AI and the Internet of Things (IoT) present new security challenges, and cyber warfare is becoming more common.
- Preventative Measures: Educating users, using advanced security technologies, and having clear incident response plans are essential for combating cybercrime.

Conclusion: Cybercrime is a complex, evolving threat that requires coordinated global efforts and continuous improvement in cybersecurity measures. As technology continues to advance, staying ahead of cybercriminals will remain a significant challenge for the global community.

Cybercrime Era: Survival Mantra for the Netizens

Netizens = Net + Citizen. It refers to a citizen of internet. Netizen is someone who actively involved in online communities or the internet in general.

The 5P Netizen Mantra for online security encompasses five key principles to help users stay safe and secure in the digital world: Precaution, Prevention, Protection, Preservation, and Perseverance. Here's a brief explanation of each:

1. Precaution
   - Be Cautious: Always be mindful and alert when navigating the internet. Avoid clicking on unknown links or downloading files from untrusted sources.
   - Verify Sources: Ensure that websites and emails are legitimate before providing any personal or financial information.
   - Stay Informed: Keep yourself updated about common cyber threats and scams to recognize and avoid them.
2. Prevention
   - Strong Passwords: Use complex and unique passwords for different accounts to reduce the risk of unauthorized access.
   - Regular Updates: Keep your operating system, software, and applications updated to patch vulnerabilities.
   - Avoid Public Wi-Fi: Be cautious when using public Wi-Fi networks, as they are often insecure and can be exploited by cybercriminals.
3. Protection
   1. Antivirus Software: Install and regularly update antivirus software to detect and remove malware.
   2. Firewalls: Use firewalls to block unauthorized access to your computer or network.

4. Preservation

- **Data Backup:** Regularly back up your important data to an external drive or cloud storage to prevent loss in case of a cyber attack.
- **Secure Storage**: Ensure that backups are stored securely and can be accessed only by authorized persons.
- **Data Encryption:** Encrypt sensitive data to protect it from unauthorized access.

5. Perseverance

- **Continuous Learning:** Stay educated about the latest cybersecurity practices and threats.
- **Vigilance:** Maintain a proactive approach to security by regularly reviewing and updating your security measures.
- **Adaptability:** Be prepared to adapt and improve your security practices as new threats emerge.

Cyber Offense

A cyber offense refers to any illegal activity that involves a computer or network to commit harm, steal data, disrupt services, or exploit systems.
A cyber offense is a broader term that can include any malicious or harmful activity conducted through digital means. This can encompass actions that may not necessarily be classified as crimes under the law
While cybercrime is a subset of cyber offenses and specifically refers to activities that are illegal.

Example of a Cyber Offense : Doxing
Doxing is the act of publicly revealing private or personal information about an individual without their consent, typically with the intent to harass, intimidate, or embarrass them.

- Collection of Information: Gathering personal details such as home addresses, phone numbers, email addresses, and social security numbers from various sources.
- Public Disclosure: Sharing this collected information on public forums, social media, or websites.
- Intent to Harm: Aimed at causing distress, fear, or harm to the individual targeted.

How criminals plan the Attacks

The cyber attack life cycle, also known as the cyber kill chain, describes the stages a hacker goes through to carry out a successful attack. Here's a simple explanation with an example:

1. Reconnaissance (Survey)

The hacker gathers information about the target. This can be done by looking up publicly available information, scanning for vulnerabilities, or using social engineering to learn more about the target. Two types of reconnaissance are active and passive reconnaissance.

Example: A hacker searches for an employee's email address on the company's website and checks their social media for more details.

2. Weaponization (Preparation)

The hacker creates or assembles tools to exploit the target's weaknesses. This could be malware, phishing emails, or other types of attack software.

Example: The hacker crafts a fake email that looks like it's from a trusted source and attaches malware to it.

3. Delivery

The hacker sends the weapon to the target. This can be done through email, malicious websites, or infected USB drives.

Example: The hacker sends the fake email with malware to the employee's email address.

4. Exploitation (Break-in)

The weapon exploits a vulnerability in the target’s system to gain access. This could be a software flaw or a human error, like clicking on a malicious link.

Example: The employee opens the email and clicks on the attachment, which installs malware on their computer.

5. Installation

The hacker installs malicious software on the target system to maintain access and control.

Example: The malware creates a backdoor on the employee's computer, allowing the hacker to access it remotely.

6. Command and Control (Control)

The hacker establishes a communication channel with the compromised system to control it and gather data.

Example: The backdoor malware connects to the hacker's server, allowing the hacker to send commands and receive information from the employee's computer.

7. Actions on Objectives (Steal Data or Disrupt)

The hacker achieves their goals, such as stealing data, disrupting operations, or further spreading the malware.

Example: The hacker steals sensitive company information from the employee's computer or uses it to launch further attacks within the organization

Stages of Cyber Attack Lifecycle

1. Reconnaissance

Scanning the environment or harvesting information from social media.

2. Weaponization

Pairing malicious code with an exploit to create a weapon (piece of malware).

3. Delivery

Transmission of weapon/malware to target (e.g. via email, USB, website).

4. Exploitation

Once delivered, the weapons/malware code is triggered upon an action. This in turn exploits the vulnerability.

5. Installation

The weapon installs malware on the system.

6. Command and Control

A command channel for remote manipulation of the victim.

7. Action on objectives

With hands on access the attacker and achieve their objective.

Social Engineering

Social engineering is the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Two types of social engineering are as follows:

1.Human-Based Social Engineering

Human-based social engineering involves direct interaction with individuals to manipulate them into divulging confidential information or performing actions that compromise security. These techniques rely heavily on psychological manipulation and exploiting human trust and social norms.

Techniques of Human-Based Social Engineering

- Impersonation : The attacker pretends to be someone else, such as a coworker, authority figure, or IT support, to gain trust and extract information. Eg: An attacker poses as an IT technician and asks employees for their passwords to "fix" an issue.
- Tailgating: The attacker gains physical access to a restricted area by following someone with legitimate access. Eg: An attacker waits for an employee to use their access card and then slips in behind them without using a card.
- Shoulder Surfing :The attacker observes someone entering sensitive information, such as passwords or PINs, by looking over their shoulder. Eg: An attacker watches someone enter their ATM PIN or computer login credentials in a public place.
- Quid Pro Quo :The attacker offers something in return for information or access. Eg: An attacker offers free software or services in exchange for login credentials.

2. Computer-Based Social Engineering

Computer-based social engineering exploits digital communication channels to deceive individuals into providing sensitive information or performing compromising actions. These attacks often use technology to amplify the reach and effectiveness of the fraud.

Techniques of Computer-Based Social Engineering

- Phishing: The attacker sends fake emails or messages designed to appear legitimate, tricking user into providing personal information or clicking on malicious links. Eg: An email that appears to be from a bank asking the user to verify their account information.
- Spear Phishing: A targeted form of phishing where the attacker customizes the message for a specific individual or organization. Eg: An email that appears to come from a colleague, referencing a specific project or event.
- Smishing: Similar to phishing , but using SMS or text messages to deceive the user. Eg: A text message claiming to be from a delivery service asking the user to click a link to track their package.
- Vishing: Voice phishing where the attacker uses phone calls to deceive victims into revealing sensitive information. Eg: A phone call from someone pretending to be from tech support, asking for login credentials.
- Baiting: The attacker trap the target with something appealing, such as free downloads or gifts, to induce them into a trap. Eg: A website offering free music downloads that, when clicked, installs malware on the user's computer.
- Malware: The attacker uses malicious software to gain unauthorized access to systems or data. Eg: A user unknowingly downloads and installs software that logs their keystrokes, capturing sensitive information

Cyber Stalking

Cyber stalking is a form of harassment that takes place online. It involves using the internet, social media, emails, or other digital communication methods to repeatedly harass, threaten, or intimidate someone.

Cyber stalking is when someone uses technology to follow, monitor, or harass another person. This can happen through:

- Social Media: Sending unwanted messages, commenting aggressively, or tracking someone's activities.
- Emails and Messages: Bombarding someone with threatening or unwanted emails, texts, or direct messages.
- Websites and Blogs: Creating websites or blogs to spread false information or to target the victim.
- Spyware: Installing software on someone's device to monitor their activities without their knowledge.

Key Characteristics of Cyber Stalking

1. **Persistent Contact:** The stalker repeatedly tries to communicate with the victim, even after being asked to stop.
2. **Threatening Behavior:** The stalker might send threats, making the victim feel scared or unsafe.
3. **Monitoring Activities**: The stalker keeps a close watch on the victim's online activities, such as their posts, friends, and locations.
4. **Impersonation:** The stalker might pretend to be someone else to gain information about the victim or to harm their reputation.
5. **Spreading False Information:** The stalker might spread rumors or lies about the victim online to damage their reputation.
6. **Privacy Invasion**: The stalker might hack into the victim's accounts or devices to steal personal information.
7. **Legal Consequences:** In many places, cyber stalking is a crime, and victims can seek help from law enforcement.

Cybercafe

A cybercafe, also known as an internet cafe, is a place where people can pay to use computers with internet access.

- Location: A physical space, such as a shop or a dedicated area in a larger establishment.
- Services: Offers computers and internet access to customers for a fee. Some cybercafes also provide additional services like printing, scanning, and gaming.

How Does a Cybercafe Work?

1. Access: Customers enter the cybercafe and pay for the amount of time they wish to use a computer. Payment can be by the hour, half-hour, or in smaller time increments.
2. Usage: Once they have paid, customers are assigned a computer. They can use the internet to browse websites, check email, use social media, or any other online activity.
3. Additional Services: Some cybercafes offer additional services such as:
    - Printing and Scanning: Customers can print documents or scan papers.
    - Gaming: Many cybercafes have computers equipped with popular games, attracting gamers who want to play online.
    - Software Access: Access to specialized software that customers might not have on their personal computers.

Why Do People Use Cybercafes?

- No Personal Computer: People without a personal computer or internet access at home can use the services.
- Travel: Travelers who need to check email or access the internet.
- Convenience: Convenient for those who need to use a computer temporarily, such as for printing a document.
- Gaming: Gamers who want to play on high-performance computers with fast internet connections.

Role of Cybercafe in Cybercrime

1. Anonymity:

- Anonymity: Cybercafes provide a level of anonymity that cybercriminals can exploit. Users can access the internet without revealing their true identities, making it difficult to trace illegal activities back to them.
- Temporary Presence: Since usage is often brief and customers frequently change, it is challenging to maintain records of who did what and when.

2. Access Point for Illegal Activities:

- Phishing and Hacking: Cybercriminals can use cybercafe computers to send phishing emails, conduct hacking operations, and execute other cyber attacks without fear of being easily traced.
- Fraud Transactions: Activities like online fraud, using stolen credit card information, or setting up fake accounts can be conducted from cybercafes to avoid detection.

3. Launching Attacks:

- DDoS Attacks: Cybercafes can be used to initiate Distributed Denial of Service (DDoS) attacks. Cybercriminals can use the cafe's network to send massive amounts of traffic to target websites, overwhelming them and causing them to crash.
- Botnet Operations: Cybercafes can serve as command centers for botnets. Cybercriminals can control networks of infected computers (bots) from a cybercafe, coordinating large-scale cyber attacks.

4. Illegal Content Distribution:

- Piracy: Cybercafes can be used to download or distribute pirated software, movies, music, and other illegal content.
- Malware Distribution: Cybercriminals can use cybercafes to spread malware, infecting other systems by sending malicious emails or hosting infected files.

5.Money Laundering and Financial Crimes:

- Cryptocurrency Transactions: Cybercafes can be used to conduct various cryptocurrency transactions, which can be part of money laundering schemes or used to pay for illegal services.
- Financial Fraud: Conducting financial fraud, such as online banking transactions or money transfers, can be done from cybercafes to hide their identity.

Preventive Measures

1. Always logout: While checking E-Mails or logging into chatting services such as instant messaging or using any other service that requires a username and a password, always click "logout" or sign out" before leaving the system.

2. Stay with the computer: While surfing/browsing, one should not leave the system unattended for any period of time. If one has to go out, logout and close all browser windows.

3. Clear history and temporary files: Internet Explorer saves pages that you have visited in the history folder and in temporary Internet files . Your passwords may also be stored in the browser if that option has been enabled on the computer that you have used.

4. Be alert: One should have to stay alert and aware of the surroundings while using a public computer. Snooping over the shoulder is an easy way of getting your username and password.

5. Avoid online financial transactions: Ideally one should avoid online banking, shopping or other transactions that require one to provide personal, confidential and sensitive information such as credit card or bank account details.

6. Change password

7. Virtual keyboard: Nowadays almost every bank has provided the virtual keyboard on their website.

8. Security warnings: One should take utmost care while accessing the websites of any banks/financial institution.

Botnet

A botnet (short for "robot network") is a network of computers that have been infected with malware and are controlled as a group without the owners' knowledge. These infected computers, often referred to as "bots" or "zombies," can be remotely managed by a hacker or group of hackers, known as the "bot herder" or "botmaster." Botnets are typically used for various malicious activities, such as sending spam emails, launching Distributed Denial of Service (DDoS) attacks, and spreading other types of malware.

How Botnets Work

1. Infection: Botnets are created when computers are infected with malware. This can happen through various means, such as phishing emails, malicious downloads, or vulnerabilities in software.
2. Communication: Once infected, the bot communicates with a command-and-control (C&C) server controlled by the botmaster. This server sends instructions to the bot and can receive data from it.
3. Execution: The bots carry out the commands sent by the botmaster. This can include sending spam, stealing personal information, or participating in coordinated attacks.

Why Botnets are Considered Fuel for Cybercrime?

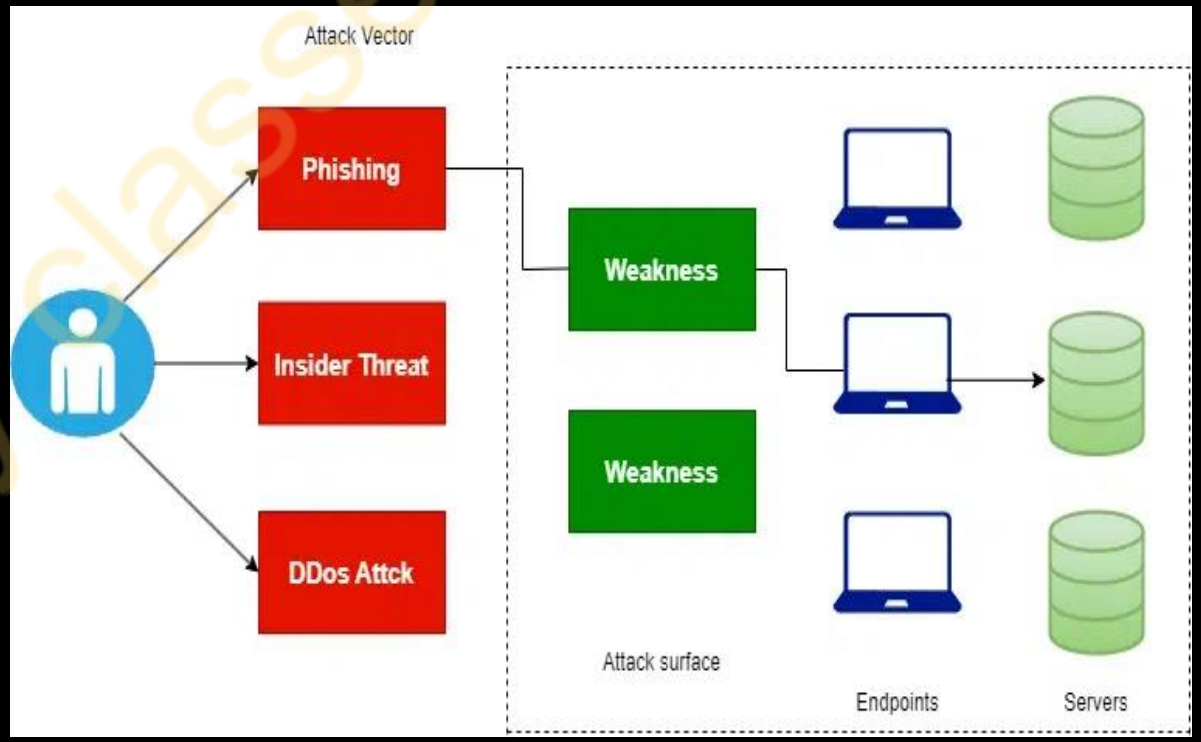
1. Anonymity and Scale: Botnets allow cybercriminals to conduct large-scale operations while remaining anonymous. The use of multiple infected computers helps hide the attack's origin and makes it more challenging to trace back to the offender.
2. Distributed Power: By harnessing the power of many computers, botnets can carry out attacks that would be impossible for a single computer. For example, DDoS attacks use thousands of bots to flood a target with traffic, overwhelming its resources and causing it to crash.
3. Monetization: Botnets can be used for various profitable cybercrimes. They can send massive amounts of spam emails, generate click fraud, steal sensitive information for identity theft.
4. Flexibility: Botnets are versatile tools that can be repurposed for different types of attacks. Once a computer is part of a botnet, it can be used for anything the botmaster desires, making it a valuable asset in the cybercriminal's toolkit.
5. Resilience: Modern botnets are designed to be resilient to shutdown efforts. They often use decentralized architectures and multiple C&C servers, making it difficult for authorities to dismantle the entire network.

Examples of Botnet Uses in Cybercrime

1. DDoS Attacks: Overwhelming websites or online services to make them unavailable to users.
2. Spam Campaigns: Sending out large volumes of unsolicited emails, often containing phishing attempts or malware.
3. Data Theft: Stealing personal information, credit card details, and other sensitive data from infected computers.
4. Click Fraud: Generating fake clicks on online ads to deceive advertisers and generate illegal revenue.
5. Crypto jacking: Using the infected computers processing power to mine cryptocurrencies without the owner consent.

Attack Vector

Attack vectors are the specific paths or methods that cyber attackers use to gain unauthorized access to a system, network, or application. These vectors serve as entry points for attacks, allowing malicious actors to exploit vulnerabilities. Every ethical hacker has their unique attack vector to check the security of the target application, this application may be a web application or an android application.



Common Attack Vectors

1. Phishing:

Attackers send deceptive emails or messages designed to trick recipients into divulging sensitive information, such as login credentials or financial information.

Example: An email that appears to be from a trusted source (like a bank) asking the recipient to click a link and enter their account details.

2. Malware:

Malicious software designed to disrupt, damage, or gain unauthorized access to a computer system. Malware Includes viruses, worms, Trojans, ransomware, spyware, and adware.

Example: Ransomware encrypts the victim's files and demands payment for the decryption key.

3. Social Engineering:

Manipulating individuals into performing actions or divulging confidential information. Techniques includes baiting, quid pro quo, and tailgating.

Example: A phone call pretending to be from tech support, asking for login details.

4. Exploiting Vulnerabilities:

Taking advantage of flaws or weaknesses in software or hardware. Common Vulnerabilities includes Unpatched software, outdated systems, and zero-day vulnerabilities.

Example: An attacker exploiting an unpatched software vulnerability to gain control of a system.

5.Denial of Service (DoS) and Distributed Denial of Service (DDoS):

Attacks aimed at making a machine or network resource unavailable to its intended users by overwhelming it with a flood of illegitimate requests.

Example: A DDoS attack that sends massive amounts of traffic to a website, causing it to crash.

Difference b/w Attack Vector and Attack Surface

Aspect	Attack Vector	Attack Surface
Definition	The specific method or path used by an attacker to gain access.	The total sum of all possible entry points an attacker can use.
Scope	Individual techniques or paths.	Overall collection of potential vulnerabilities.
Focus	How an attack is carried out.	Where an attack can be carried out.
Examples	Phishing, malware, exploiting software bugs.	Open ports, software interfaces, user accounts.
Analogy	A single door or window a thief uses.	All doors, windows, and entry points of a house.

PAPER ID-311222

Roll No.

Printed Page: 1 of 1
Subject Code: BCC301

BTECH
(SEM III) THEORY EXAMINATION 2023-24
CYBER SECURITY

TIME: 3HRS **M.MARKS: 70**

Note: 1. Attempt all Sections. If require any missing data; then choose suitably.

SECTION A

1. Attempt *all* questions in brief.

Q no.	Question	Marks
a.	Define Cyber Crime.	2
b.	What is Bot net.	2
c.	Why mobile needs security?	2
d.	Define Authentication and Authorization.	2
e.	What is virus and worms.	2
f.	Explain digital evidence?	2
g.	Why cyber is needed?	2

SECTION B

2. Attempt any *three* of the following:

a.	Explain how the term 'cybercrime' originated. State few Cyber Crimes.	7
b.	Explain wireless devices with example. What are the security challenges faced by wireless devices?	7
c.	Explain 7 Tools used in Cyber Crime.	7
d.	Explain Digital forensics life cycle.	7
e.	What is the need of Information Security policy?	7

SECTION C

3. Attempt any *one* part of the following:

a.	Who are Cyber Criminals? Classify Cybercrimes.	7
b.	What is the fuel for cybercrime. How may a criminal plan cybercrime?	7

4. Attempt any *one* part of the following:

a.	Explain the security measures and policies taken for mobile devices.	7
b.	State some attacks on Mobile devices. What are the security implications for organizations.	7

5. Attempt any *one* part of the following:

a.	What is Identity Theft. How it is done and how ID Theft can be handled?	7
b.	What is steganography. Explain in detail.	7

6. Attempt any *one* part of the following:

a.	What is Email. Explain how Email forensics can be done.	7
b.	What are privacy threats? What are the challenges faced?	7

7. Attempt any *one* part of the following:

a.	What is Cyber Law. State a few Cyber law in India.	7
b.	Give a Overview of Intellectual Property related Legislation in India.	7

Important Question

2 marks questions

Q.1 What is cybersecurity? Why we need it?

Q.2 Define the term Cybercrime?

Q.3 Who are Cybercriminals?

Q.4 What is information security?

Q.5 What is Botnet?

Q.6 Define the term attack vector?

7 marks questions

Q.1 Discuss the survival mantra for netizens?

Q.2 What is cybercrime? Explain the classification of cybercrime?

Q.3 Who are cybercriminal? Discuss the types of cybercriminals? How cybercriminals plan their attack?

Q.4 What is Botnet? How its work as a fuel for cybercrime?

Q.5 What is social engineering? Also discuss the types of social engineering?

Thank You