Types of Cyber Crimes and Offenses

- ## Categorization

    a. **By Target**
        - **Individuals**
            - Crimes like phishing, cyberstalking, identity theft, and cyber defamation target personal data, privacy, or reputation.
            - Example: Sending fake emails to steal login credentials.
        - **Property**
            - Focus on digital or intellectual assets, such as credit card fraud, intellectual property theft, or cyber vandalism.
            - Example: Unauthorized use of someone's internet connection (internet time theft).
        - **Organizations**
            - Target businesses or institutions through unauthorized access, Denial-of-Service (DoS) attacks, malware, or data theft.
            - Example: Overloading a company's servers to disrupt services.

    b. **By Nature**
        - **Single Event:**
            - One-time incidents, such as a single phishing email or a one-off hacking attempt.
            - Example: A hacker stealing credit card details in a single breach.
        - **Series of Events:**
            - Ongoing or repeated attacks, such as sustained cyberstalking or salami attacks (small, unnoticed thefts over time).
            - Example: Continuous harassment via threatening emails.

Planning Ideas Of Crime

➢ Attacks

- **Definition:**
  - Attacks are the execution phase of a cybercrime where cybercriminals exploit vulnerabilities to achieve malicious objectives such as stealing data, disrupting systems, or gaining unauthorized access.

- **Types of Attacks**
  - **Active Attacks**
    - Involves direct interaction with the target system to exploit vulnerabilities.
    - Attacker efforts to change/modify the content of messages
    - More riskier than passive attack as it triggers security alerts
  - **Passive Attack**
    - We gather information about a target without his/her knowledge
    - Done through search engines like google or yahoo, surf platforms like Instagram, Facebook or LinkedIn.
    - From websites or particular blogs/newspapers

- **How criminals plan the attacks**
  - Criminals follow a structured approach to execute cyber attacks, divided into three key phases:
    - **Reconnaissance:**
      - It is the first phase
      - Passive information gathering about the target without their knowledge, treated as a passive attack
      - **Footprinting -** Collect data about the target system or individual.
      - To identify potential vulnerabilities or entry points

    - **Scanning and Scrutinizing:**

        - Validating gathered information and identify the existing vulnerabilities in the target's systems
        - To refine the attack strategy based on verified data.

    - **Launch an attack:**
        - Executing the exploit to achieve the criminal's objective
        - To steal data, disrupt operations, or achieve other malicious goals

- **Attack Execution**
    - **Crack Passwords**: Gain initial access to systems.
    - **Exploit Privileges**: Escalate control within the system.
    - **Execute Malicious Commands/Applications**: Deploy malware or harmful scripts.
    - **Hide Files**: Conceal malicious activities to avoid detection.
    - **Cover Tracks**: Delete access logs to erase evidence.

➢ Social Engineering

- **Definition:**
    - A manipulation technique that exploits human error to gain private information, access, or valuables.
    - In cybercrime, it involves "human hacking" scams that trick unsuspecting users into exposing data, spreading malware, or granting access to restricted systems.
    - Attacks can occur online, in-person, or through other interactions.

- **Classification:**
    - **Human based:**
        - Impersonating employees or valid users.
        - Posing as important users (e.g., CEO).
        - Using third parties to gain system access.
        - Calling technical support for information.
        - **Shoulder surfing:** Observing usernames/passwords.

- **Dumpster diving:** Collecting information from trash.

- **Computer Based:**
  - **Phishing:** Fake Emails
  - Sends email attachments with malicious code which executes when opening
  - Pop up window showing free-stuff/offers to trick users into providing data

➢ CyberStalking

- **Definition**
  - **“Stalking”:** act or process of following prey stealthily trying to approach somebody or something
  - Using the internet to threaten or harass consistently via email, social media, etc.
  - It involves using digital platforms to intimidate or control someone by continuously monitoring, sending unwanted messages or harassing them online, and tracks the victim's online activity.

- **Types of Stalkers**
  - **Online**
    - Aim to start interaction with victims directly through the internet.
    - Emails and chat rooms are the most popular communication medium to get connected with victims rather than traditional methods.
    - Stalker makes sure the victim recognizes the attack attempted on him/her.
    - Can make use of a third party to harass the victim

  - **Offline**
    - Stalkers attack the victim using traditional methods like following the victim or watching their daily routine.
    - Common way to gather information about victims is done through the internet.

- **How Stalking Works?**
  - Collecting personal information like name, number, address, date of birth of the victim.
  - Establish contact through telephone.
  - Once contact is established, the stalker calls the victim to threaten/harass.
  - Stalkers almost always establish contact through email which can be in tone of loving, threatening or can be sexually explicit.
  - Stalker may use multiple names while contacting
  - Some stalkers send repeated emails asking for various kinds of favors from the victim.

➢ CyberCafes

- **Definition:**
  - Cybercafes, as public computer access points, are often exploited for cybercrimes due to their accessibility and anonymity
  - Often used to send obscene emails to harass someone.

- **Risks:**
  - **Malicious Programs**: Keyloggers or spyware may capture passwords and sensitive data.
  - **Over-the-Shoulder Surfing**: Attackers observe users to steal credentials.

- **Legal Perspective (India):**
  - Under the **Information Technology Act, 2000**, cybercafes are "network service providers" in **Section 79**, which imposes them a responsibility of due diligence, which if failed will be liable for offense.
  - Cybercriminals prefer carrying out their work in cybercafes.

- **Survey Findings:**
  - Pirated softwares is installed in the computers.
  - Antivirus software is not of the latest version or patch.

- Pornographic sites with indecent contents were not blocked.
- Several computers have **"Deep Freeze",** that protects the computers from prospective malware attacks by wiping out details of all activities carried out in the computer when clicked restart button.
- Owner has very low awareness of IT and IT governance.
- Cyber cell wings do not seem to conduct periodic visits.

- **Safety Tips:**
  - Always log out
  - Clear browsing history
  - Avoid financial transactions
  - Use virtual keyboards
  - Change Passwords
  - Stay with the computer & be alert
  - Keep an eye on security warnings

➢ Botnets

- **Definition:**
  - A collection of software robots (bots) that run autonomously and automatically
  - An automated program for doing some particular task
  - Bots infect computers via viruses or malicious code, granting attackers remote access.
  - Used for tasks like sending spam, launching DoS attacks, or mining cryptocurrency.

- **Security Measures:**
  - Use updated antivirus/anti-spyware software.
  - Enable automatic OS security patches.
  - Install firewalls
  - Disconnect from the internet when not in use.
  - Download from trusted sites
  - Monitor mailboxes

- Immediate action if system is infected

➢ Attack Vector

- **Definition:**
  - A path which an attacker uses to gain unauthorized access to a computer to deliver a malicious outcome

- **Types:**
  - **Technological:** Viruses, email attachments, webpages, pop-up windows, instant messages, chat rooms.
  - **Human-Based:** Deception, where users are tricked into weakening system defenses (e.g., via social engineering)

- **Common Payloads**: Viruses, Trojan horses, worms, spyware

- **Specific Vectors:**
  - **Attack by Email:**
    - The content is either embedded in the message or linked to by the message.
    - Sometimes attacks combine the two vectors, so that if the message does not get you, the attachment will.
    - Spam emails carry fraud, scams or malware.
  - **Attachments (and other files):**
    - Malicious attachments install malicious code which could be virus, trojan horse, spyware or any other.
    - Attempts to install as soon as we open the attachments.
  - **Attack by deception:**
    - Aimed at the user/operator as an entry point.
    - It is not just malicious code that one needs to monitor.
    - Social engineering is done to exploit humans to gain access. Eg:- Phishing.
    - Scams and Frauds require user cooperation to succeed
  - **Hackers:**

- Hackers/crackers are formidable attack vectors as people are flexible and can improvise.
- Use tools, heuristics, and social engineering to install Trojan horses to gain control.

➢ Cloud Computing

- **Definition:**
  - Internet-based delivery of hosted services, providing on-demand computing resources.
  - It is internet-based development and use of computer technology.
  - Growing popularity of this and virtualization among organizations have made it the next target of cybercriminals.

- **Characteristics:**
  - **On-Demand:** Services are sold by usage (e.g., per minute or hour).
  - **Elastic:** Users can scale services up or down as needed.
  - **Provider-Managed:** Requires only a PC and internet connection.

- **Benefits:**
  - **Accessibility:** Data and applications are available anywhere, anytime. Data may not be held on a particular hard drive.
  - **Cost Savings:** Reduces hardware and physical infrastructure costs.
  - **IT Support:** Organizations do not need to rent physical space to store servers and databases. They just have to ensure a desktop and a continuous internet connection.

- **Types of Services:**
  - **Infrastructure-as-a-service (IaaS):**
    - Provides virtual servers with unique IP addresses and blocks of storage on demand like Amazon Web Service.
    - Offers APIs from which customers can control their servers.

- Users just need to pay for exactly the amount of service they used. It is also called utility computing

- **Platform-as-a-service (PaaS):**
  - It is a set of software and development tools hosted on a provider's server. Can also create applications through the provider's APIs.
  - Google Apps is one of the most famous PaaS providers.
  - Some providers may not allow you to take your applications and put it on another platform.

- **Software-as-a-service (SaaS):**
  - It is the broadest market.
  - Provider allows customers to only use its application.
  - Software interacts with the user through the user interface.
  - These apps can be anything like web based e-mails to social media platforms like twitter.

- **Risks:**

1. Elevated user access	Any data processed outside the organization brings with it an inherent level of risk
2. Regulatory compliance	Cloud computing service providers are notable and/or not willing to undergo external assessments.
3. Location of the data	User doesn't know where the data is stored or in which country it is hosted.
4. Segregation Of Data	Data of one organization is scattered in different locations
5. Recovery Of Data	Incase of any disaster, availability of the services And data is critical.
6. Information security violation reports	Due to complex IT environment and several customers logging in & out of the hosts, it becomes difficult to trace inappropriate and/or Illegal activity
7. Long-term viability	In case of any major change in the cloud computing service provider(eg: acquisition/ merger/partnership/breakage), the service provided is at stake.

CyberCrime Targeting Devices

➢ Computers, Mobiles and Wireless Devices

- Increased use of mobile devices (smartphones, tablets) for activities like gaming, email, and banking makes them prime targets.

- **Types of mobile computers:**

  - **Portable Computer:**
    - General-purpose, can easily move from one place to another
    - Cannot be used in transit as it requires setup and AC power.
  - **Tablet PC:**
    - A slate-shaped device with a touchscreen, stylus, and handwriting recognition, lacking a physical keyboard.
  - **Internet Tablet:**
    - Internet appliance in tablet form.
    - It has limited computing power & restricted application suite.
  - **Personal Digital Assistant (PDA):**
    - Small, pocket-sized with limited functionality synchronize with desktops for contacts, emails, and notes.
  - **Ultra-Mobile PC:**
    - A PDA-sized, full-featured computer running a general-purpose OS.
  - **Smartphone:**
    - PDA with an integrated cell phone functionality having a wide range of features and installable applications.
  - **Carputer:**
    - An in-car computing device serving as a wireless computer, sound system, GPS, DVD player & Bluetooth-enabled system.
  - **Fly Fusion Pentop:**
    - A pen-sized device functioning as a writing tool, MP3 player, language translation, storage device, and calculator.

- **Attacks on 3G Mobile Networks**

  - **Malware, Viruses, and Worms:**
    - **Skull Trojan**:
      - Targets symbian OS series 60 phones.
    - **Cabir Worm**:
      - 1st dedicated mobile phone worm infects a phone with Symbian OS.
      - It scans other devices and sends a copy of itself to the first vulnerable phone, spreads via Bluetooth
      - The worst thing is that Cabir-H and Cabir-I source codes are publicly available.
    - **Mosquito Trojan**:
      - Affects Series 60 smartphones
      - Name came from a cracked version of the “Mosquitos” game.
    - **Brador Trojan**:
      - Targets Windows CE OS by creating svchost.exe file in start-up folder which takes full control of the device.
    - **Lasco Worm**:
      - First released in 2005
      - Target PDAs and phones running on symbian OS.
      - It is based on Cabir’s source code and spreads via Bluetooth.

  - **Denial-of-Service (DoS):**
    - The main objective is to make the system unavailable to intended users.
    - Virus aims to make systems unavailable.
    - One of the most common threats to wired internet service providers(iSPs) is DDoS attacks which are used to flood the target system with the data so that the response from the target system is either slowed or stopped.

- **Overbilling Attack:**
  - Hijacks a subscriber's IP address and then uses it to initiate downloads which are not free and use it for his/her purpose.

- **Spoofed Policy Development Process (PDP):**
  - Exploits vulnerabilities in GTP [General Packet Radio Service (GPRS) Tunneling Protocol].

- **Signaling-Level Attacks:**
  - Targets Session Initiation Protocol (SIP), a signaling protocol used in IP multimedia subsystem (IMS) networks to provide Voice over Internet Protocol(VoIP) systems, exploiting vulnerabilities.

➢ Cyber Crime Against Women

- Cyber violence uses technology to access women's personal information and harass or exploit them.
- Affects women by subjecting them to mental and emotional harassment.
- Most women become distressed and depressed under this type of crime.

- **Types:**
  - **Cyberstalking:**
    - Threatening messages or unwanted contact via social media to cause distress.
  - **Cyber Defamation:**
    - Involves defaming a victim through blackmailing or disclosing altered images to defame victims.
  - **Cyber Hacking**:
    - Tricking women into clicking malicious links or apps that leak personal data becoming victims of cyber hacking.
  - **Cyber Bullying:**
    - Regular harassment and bullying victims with abusive content, threats, or misleading posts and sending rape/death threats.

- **Pornography:**
  - Involves posting morphed images of victims and using them for pornographic purposes, often demanding money to remove them.
- **Cyber Grooming:**
  - Building online relationships to manipulate and pressurizes women into sexual acts or undue favors.

➢ Cybercrime in Finance

- **Definition:**
  - Act of obtaining financial gain through profit-driven criminal activity like identity fraud, ransomware attacks, email/internet fraud, and attempts to steal payment card information.

- **Activities:**
  - Stealing payment card information or accessing financial accounts for unauthorized transactions
  - Extortion
  - Identity fraud to apply for financial products

- **Impact:**
  - Heavily targets the lucrative financial services industry but also affects companies and individuals.

➢ Social Engineering Attacks

- **Baiting**: Attacker lures users into a trap with false promises (e.g., free gifts) to install malware.
- **Malware Scams**: Tricks users into believing that malware is installed and makes them pay to remove fake malware.
- **Pretexting**: Uses fake identities and scenarios to extract information.
- **Tailgating**: Gains unauthorized physical access by following employees.

- **Phishing**: Fake emails, websites, or texts to steal data (mass targeting).
- **Smishing**: Phishing via SMS.
- **Spear Phishing**: Targeted phishing against specific individuals or companies.
- **Vishing**: Voice-based phishing using phone calls or voicemails, sometimes with voice changers.

➢ Malware and Ransomware Attacks

- **Malware:**
  - Malicious software that harms devices by locking them, stealing/encrypting data, or attacking other systems.
    - Steals/deletes data
    - Taking control of devices
    - Mining cryptocurrencies
    - Using services that cost us money
    - Causes devices to be locked or unusable.

- **Ransomware:**
  - Ransomware is a type of malware that prevents you from accessing your computer where the computer becomes locked or data on it might get stolen or deleted.
  - Some ransomwares spread to other machines on the network like **Wannacry malware** impacted the **NHS in May 2017**.
  - Usually asks to conduct an attack through emails or follow instructions on an anonymous web page to make payment.
  - Payment is done in cryptocurrencies in order to unlock computers or access our data. However, even if we pay no guarantee that we will get access to computers.

➢ Zero Day Attack

- **Definition:**
  - A security risk in a piece of software that is not publicly known and the vendor not aware of.
  - Method an attacker uses to access the vulnerable system.
  - A zero day attack is so-called because it occurs before the target is aware that the vulnerability exists. The attacker releases malware before the developer or vendor has had the opportunity to create a patch to fix the vulnerability.
  - A pirated version of a movie, music, or software is referred to as "zero day" when it becomes available at the same time or before the official release.
  - In other words, the pirated version is published zero days after the official version.
  - A zero-day attack begins with a hacker discovering a zero-day vulnerability, which is an error in code or software that the target has yet to discover.
  - Attacker takes advantage of existing vulnerability and does zero-day exploit.

- **How Zero Day Works:**
  1. **Vulnerability Introduced**: Developer creates software with unknown flaws.
  2. **Exploit Released**: Attackers discover and exploit the vulnerability before a fix.
  3. **Vulnerability Discovered**: The vendor learns of the flaw but lacks a patch.
  4. **Vulnerability Disclosed**: Public announcement alerts users and attackers.
  5. **Antivirus Signatures Released**: Vendors identify and block malware targeting the vulnerability.
  6. **Security Patch Released**: Vendor fixes the flaw, but deployment takes time.

7. **Patch Deployment Completed**: Users must apply the patch, often delayed without auto-updates.