**Chapter 2 :- Cyber offenses and Cyberstalking**

2.1 Criminals Plan: Categories of Cybercrime Cyber Attacks: Reconnaissance, Passive Attack, Active Attacks, Scanning/Scrutinizing gathered Information, Attack (Gaining and Maintaining the System Access), Social Engineering, and Classification of Social Engineering. 2.2 Cyberstalking: Types of Stalkers, Cases Reported on Cyberstalking, Working of Stalking 2.3 Real-Life Incident of Cyber stalking 2.4 Cybercafe and Cybercrimes 2.5 Botnets: The Fuel for Cybercrime, Botnet, Attack Vector 2.6 Cybercrime: Mobile and Wireless Devices – Proliferation - Trends in Mobility 2.7 Credit Card Frauds in Mobile and Wireless Computing Era 2.8 Security Challenges Posed by Mobile Devices 2.9 Authentication Service Security 2.10 Attacks on Mobile/Cell Phones

**2.1 Criminal Plan:**

Cybercrime encompasses a wide range of illegal activities conducted via computers or networks. Understanding the categories and types of cybercrime is crucial for prevention and response strategies. Below is a detailed overview of the various categories of cybercrime and types of cyber attacks, including reconnaissance, passive and active attacks, and social engineering.

 **Categories of Cybercrime**

Cybercrime can be broadly classified into four main categories:

1. Individual Cyber Crimes: These crimes target individuals and include activities such as phishing, spoofing, and cyberstalking.

2. Organizational Cyber Crimes: These crimes are aimed at organizations and often involve coordinated attacks by groups. Common examples include malware attacks and denial-of-service (DoS) attacks.

3. Property Cyber Crimes: This category includes crimes that target property, such as credit card fraud and intellectual property theft.

4. Societal Cyber Crimes: This is a more severe form of cybercrime that includes cyber-terrorism, which poses threats to public safety and national security.

**Types of Cyber Attacks**

Cyber attacks can be categorized based on their methods and objectives. Here are the primary types:

1. **Reconnaissance**: This is the initial phase where attackers gather information about their target. Techniques include:

Scanning/Scrutinizing: Identifying active devices on a network and assessing their vulnerabilities.

 **2. Passive Attacks:** These attacks involve monitoring or intercepting communications without altering the data. Examples include eavesdropping on network traffic.

 **3. Active Attacks:** In contrast to passive attacks, active attacks involve direct interaction with the target system to disrupt services or manipulate data. Examples include:

* Denial-of-Service (DoS) Attacks: Flooding a network with excessive requests to render services unavailable.
* Malware Attacks: Involving malicious software like viruses and ransomware that compromise system integrity.

**4. Social Engineering:** Social engineering exploits human psychology to gain unauthorized access to systems or data. Common tactics include:

* Phishing: Deceptive emails or messages designed to trick users into revealing sensitive information.
* Vishing and Smishing: Voice and SMS phishing attacks that aim to extract personal information over the phone or via text messages.

 **5. Classification of Social Engineering Attacks**

Social engineering attacks can be classified into several types:

* Spear Phishing: Targeted phishing attacks aimed at specific individuals or organizations.
* Whaling: A form of spear phishing that targets high-profile individuals, such as executives.
* Pretexting: Creating a fabricated scenario to obtain information from a victim.
* Baiting: Offering something enticing to lure victims into a trap, such as free software that contains malware.

**2.2 Cyberstalking: Types of Stalkers, Cases Reported on Cyberstalking, Working of Stalking**

Cyberstalking is a form of harassment that utilizes electronic means to stalk or intimidate an individual. It can manifest in various ways and is characterized by malicious intent, often causing significant distress to victims. Below is an overview of the types of stalkers, reported cases, and the workings of cyberstalking.

**Types of Stalkers**

1. **Online Stalking (Cyberstalking)**

Characteristics

* **Medium**: Utilizes digital platforms such as social media, email, and websites to harass and intimidate victims.
* **Methods**: Common tactics include sending unwanted messages, creating fake profiles, monitoring online activities, hacking accounts, and spreading false information. Cyberstalkers often employ anonymity to evade detection, which can embolden their behavior.
* **Scope**: Cyberstalking can escalate to offline threats, making it a serious concern for personal safety. Victims may feel constantly monitored and vulnerable due to the pervasive nature of online harassment.
* **Legal Framework**: While many jurisdictions are beginning to recognize cyberstalking as a crime, legal responses can vary significantly. Victims may face challenges in obtaining protection due to the digital nature of the harassment.
1. **Offline Stalking**

Characteristics

* **Medium**: Involves direct, physical harassment, such as following the victim, showing up at their home or workplace, or making in-person threats.
* **Methods**: Tactics may include surveillance, unwanted phone calls, and physical confrontations. Offline stalkers are typically more visible, which can heighten the immediate danger to victims.
* **Visibility**: The physical presence of an offline stalker can create a more intense sense of fear and urgency compared to online stalking, as the threat is tangible and immediate.
* **Legal Framework**: Offline stalking is often easier to report and prosecute due to the direct nature of the harassment. Victims can seek restraining orders and involve law enforcement more readily.

 **Reported Cases of Cyberstalking**

Cyberstalking cases have been on the rise, often escalating without intervention. For instance, the case of Gary Dellapenta involved him creating fake ads to facilitate the sexual assault of his victim after being rejected romantically. This case highlighted the severe implications of cyberstalking and led to California being the first state to criminalize such behavior.

Statistics indicate that in about 75% of cyberstalking cases, the situation worsens without timely intervention, underscoring the need for awareness and protective measures.

 **Working of Cyberstalking**

Cyberstalking typically involves several tactics aimed at harassing or controlling the victim:

* Monitoring Online Activities: Stalkers may track their victims' online behavior, gathering personal information through social media and other platforms.
* Sending Unwanted Communications: This can include emails, messages, and threats, often designed to intimidate or manipulate the victim.
* Creating False Profiles: Stalkers may impersonate their victims online, spreading misinformation or engaging in deceptive practices to further harass them.
* Encouraging Third-Party Harassment: Some stalkers may incite others to join in the harassment, using social media to rally support against the victim.
* Spying and Location Tracking: Utilizing technology such as GPS or spyware, stalkers can monitor the victim's physical movements and online activities, enhancing their control over the situation.
	1. **Real-Life Incident of Cyber stalking**

**1. Amy Boyer’s Case (1999)**

In 1999, Amy Boyer became a tragic victim of cyberstalking when she was murdered by Liam Youens, a man who had developed an obsession with her since high school. Youens's fixation escalated from online harassment to real-world violence, culminating in Amy's death. This case underscored the potential for online obsessions to lead to devastating outcomes and sparked discussions about the need for stronger legal protections against cyberstalking.

**2. The MySpace Cyberstalking Case (2006)**

The case of Megan Meier, a 13-year-old girl, exemplifies the tragic consequences of cyberbullying and stalking. In October 2006, Megan was deceived by an adult neighbor who created a fake MySpace profile to befriend her, only to later turn against her. The emotional manipulation and harassment led to Megan's suicide, highlighting the profound vulnerabilities of young individuals in the digital landscape and the urgent need for protective measures in online environments.

**3. The Gamergate Incident (2014)**

The Gamergate controversy began as an online critique of video game culture but quickly escalated into a widespread harassment campaign targeting women in the gaming industry. This incident involved threats, doxxing (publishing private information), and sustained online attacks against several women, including game developers and critics. The Gamergate incident illustrated the misogynistic undercurrents in online communities and the severe impact of coordinated cyberstalking efforts.

**4. Divya Sharma’s Experience (2021)**

In a more recent case, Divya Sharma, an archaeology student, experienced cyberstalking when a random account on Instagram began liking her photos and sending unsolicited messages. Initially dismissing the behavior, she became alarmed when the stalker escalated to abusive messages and threats. Divya reported the incident to the cyber police, leading to the suspension of the stalker's account. This case reflects the rising incidence of cyberstalking during the pandemic, where online harassment became more prevalent as people turned to digital platforms for social interaction.

* 1. **Cybercafe and Cybercrimes**

**Cybercafes as Hotspots for Cybercrime**

1. **Attraction for Cybercriminals**

Cybercriminals often prefer using cybercafes to conduct illegal activities for several reasons:

* **Anonymity**: The public setting allows criminals to operate without revealing their identity, making it difficult for law enforcement to trace their actions back to them.
* **Access to Resources**: Cybercafes provide the necessary infrastructure, such as computers and internet access, which can be used to commit various cybercrimes, including hacking, phishing, and identity theft.
* **Malicious Software**: Criminals may install keyloggers or spyware on shared computers to capture sensitive information, such as passwords and bank details, from unsuspecting users.

2. **Types of Cybercrimes Committed**

Cybercafes have been associated with various cybercrimes, including:

* **Identity Theft**: Criminals can use public computers to steal personal information and commit fraud.
* **Financial Fraud**: Instances of stealing bank passwords and making unauthorized withdrawals have been reported, often facilitated by the use of malware installed on the cafe's computers.
* **Harassment and Threats**: Cybercafes have been used to send threatening or obscene emails, allowing perpetrators to hide behind the anonymity of public internet access.
	1. **Botnets: The Fuel for Cybercrime, Botnet, Attack Vector**

A **botnet** is a network of compromised devices, often referred to as "zombie" computers, controlled by a single entity known as a **bot herder**. These devices are infected with malware that allows the bot herder to remotely command them to perform coordinated tasks without the users' knowledge. The term "botnet" is derived from "robot" and "network," indicating the automated nature of the devices involved.

**Formation and Control**

1. **Infection**: Cybercriminals typically infect devices through various means, including phishing emails, malicious downloads, or exploiting software vulnerabilities. Once infected, these devices become part of the botnet.
2. **Command and Control (C&C)**: The bot herder uses a command and control server to send instructions to the infected devices, allowing for centralized management of the botnet.
3. **Execution of Tasks**: The infected devices execute commands such as sending spam, stealing data, or launching attacks, all while remaining undetected by their users.

**Attack Vectors**

Botnets are versatile and can be used for a variety of cyber attacks, including:

**1. Distributed Denial-of-Service (DDoS) Attacks**

In a DDoS attack, a botnet overwhelms a target server or network with a flood of traffic, rendering it inaccessible to legitimate users. This is achieved by directing numerous infected devices to send simultaneous requests to the target, causing it to crash or slow down significantly.

**2. Phishing Campaigns**

Botnets can automate the distribution of phishing emails, tricking users into revealing sensitive information such as passwords or credit card details. By leveraging the scale of a botnet, attackers can send millions of phishing emails, increasing the likelihood of successful breaches.

**3. Data Theft**

Botnets can be employed to steal confidential information from compromised devices. This includes keylogging (recording keystrokes) and sniffing (capturing network traffic) to gather sensitive data such as banking credentials and personal information.

**4. Spam Distribution**

A significant portion of online spam is generated by botnets. These spam messages can be used to spread malware, promote scams, or conduct fraudulent activities on a large scale.

**5. Credential Stuffing and Brute Force Attacks**

Botnets can automate attempts to log into accounts by using stolen credentials or attempting to guess passwords. This method exploits weak passwords and can lead to unauthorized access to accounts.

* 1. **Cybercrime: Mobile and Wireless Devices – Proliferation - Trends in Mobility**

The proliferation of mobile and wireless devices has significantly transformed the landscape of cybercrime, leading to new trends in mobility and security threats. As mobile devices become increasingly integral to daily life, they also present attractive targets for cybercriminals. Below is an overview of the trends in mobility and the associated cybercrime risks.

**Trends in Mobility**

1. **Increased Smartphone Usage**

The number of smartphone users has surged, with estimates indicating growth from 2.5 billion in 2016 to 3.8 billion by 2021. This widespread adoption has made smartphones a primary means for accessing the internet, leading to a corresponding rise in cybercrime targeting these devices.

2. **Integration of Mobile Devices in Daily Activities**

Mobile devices are now used for various tasks, including banking, shopping, and social networking. This integration increases the amount of sensitive personal information stored on these devices, making them lucrative targets for cybercriminals.

3. **Rise of Mobile Applications**

The proliferation of mobile applications has created new avenues for cybercrime. Many legitimate apps can harbor vulnerabilities, and malicious apps can masquerade as harmless, leading to data breaches and identity theft. Users often grant broad permissions to apps without fully understanding the implications, which can lead to unintentional data leakage.

4. **Public Wi-Fi Vulnerabilities**

The use of public Wi-Fi networks has become commonplace, but these networks are often unsecured, making them prime targets for cybercriminals. Attackers can exploit weaknesses in public networks to intercept communications and steal sensitive information. Techniques such as "evil-twin" networks further complicate security, as users may unknowingly connect to fraudulent networks.

**Cybercrime Risks Associated with Mobile Devices**

1. **Malware and Ransomware**

Mobile devices are increasingly targeted by malware, including ransomware that can lock users out of their devices until a ransom is paid. In 2014 alone, Kaspersky detected almost 3.5 million malware instances targeting mobile devices.

2. **Phishing Attacks**

Cybercriminals utilize phishing techniques specifically designed for mobile platforms, such as SMSishing, where malicious messages are sent via SMS to trick users into providing personal information. This method has gained popularity as users become more skeptical of email phishing attempts.

3. **Spyware and Data Theft**

Spyware can be installed on mobile devices without the user's knowledge, collecting sensitive information such as login credentials and financial data. This type of malware often operates in the background, making it difficult for users to detect its presence.

4. **Physical Threats**

The physical loss or theft of mobile devices poses significant risks, as these devices often contain sensitive information. If proper security measures, such as password protection, are not in place, unauthorized individuals can easily access personal and financial data

* 1. **Credit Card Frauds in Mobile and Wireless Computing Era**

The rise of mobile and wireless computing has significantly impacted credit card fraud, making it easier for cybercriminals to exploit vulnerabilities associated with these technologies. Below is an overview of how credit card fraud manifests in the mobile and wireless computing era, including prevalent methods and trends.

Credit Card Fraud in the Mobile and Wireless Computing Era

1. **Proliferation of Mobile Payments**

With the increasing use of mobile devices for transactions, mobile payment systems have become commonplace. This convenience, however, has also attracted fraudsters who exploit weaknesses in mobile payment technologies. The ease of making transactions through apps can lead to less vigilance among users, making them susceptible to fraud.

2. **Common Methods of Credit Card Fraud**

**a. Skimming**

Skimming remains one of the most prevalent methods of credit card fraud. Criminals attach skimming devices to card readers, such as ATMs or point-of-sale terminals, to capture card data during legitimate transactions. This stolen information can then be used to make unauthorized purchases or create cloned cards.

**b. Phishing**

Phishing attacks have evolved to target mobile users through SMS (smishing) and fraudulent emails. Scammers trick victims into revealing their credit card information by posing as legitimate entities, such as banks or payment service providers. This method exploits the trust of users, especially when messages appear to come from known sources.

**c. Identity Theft**

Cybercriminals often use stolen personal information to apply for credit cards under false identities. This type of fraud can occur when sensitive data is compromised through data breaches or social engineering tactics. Once they obtain a credit card, fraudsters can make unauthorized transactions, leading to significant financial losses for victims.

**d. Mobile Malware**

The prevalence of mobile malware is a growing concern. Cybercriminals can deploy malicious software that targets mobile devices, allowing them to steal credit card information directly from users. This includes keystroke logging software that records user inputs, including credit card numbers during online transactions.

3. **Trends in Credit Card Fraud**

The trends in credit card fraud reflect the changing landscape of technology and consumer behavior:

* **Increase in Online Transactions**: The shift towards online shopping and mobile payments has led to a rise in credit card fraud incidents. As more consumers rely on digital transactions, fraudsters are increasingly targeting these platforms.
* **Emergence of Contactless Payments**: While contactless payment methods enhance convenience, they also present new vulnerabilities. Fraudsters can exploit weaknesses in contactless technology to conduct unauthorized transactions if they can access the card information.
* **Regulatory Responses**: In response to the surge in credit card fraud, regulatory bodies are implementing stricter security measures. For instance, the Payment Card Industry Data Security Standard (PCI DSS) aims to protect cardholder data and reduce fraud through enhanced security protocols.

4. **Preventive Measures**

To combat credit card fraud in the mobile and wireless computing era, individuals and organizations can adopt several preventive measures:

* **Regular Monitoring**: Users should frequently check their bank statements and transaction history for any unauthorized charges.
* **Secure Payment Methods**: Utilizing secure payment options, such as virtual credit cards or payment services with strong encryption, can help protect sensitive information.
* **Awareness and Education**: Educating consumers about the risks associated with mobile payments and how to recognize fraudulent activities is crucial in preventing credit card fraud.
* **Use of Security Software**: Installing reliable antivirus and anti-malware software on mobile devices can help detect and prevent malicious attacks aimed at stealing credit card information.
	1. **Security Challenges Posed by Mobile Devices**

Here are some of the key security challenges posed by mobile devices:

1. **Device Diversity and Fragmentation**

The mobile device landscape is highly diverse, with various operating systems, versions, and manufacturers. This fragmentation makes it challenging to implement consistent security measures across all devices. Vulnerabilities in older OS versions or specific device models can be difficult to address, leaving users exposed to potential attacks.

2. **Malicious Apps and Malware**

Mobile devices are vulnerable to malicious apps and malware that can steal sensitive data, track user activity, or even take control of the device. Users may unknowingly install infected apps from untrusted sources, compromising the device's security.

3. **Data Leakage and Loss**

Mobile devices are prone to data leakage and loss due to factors such as device theft, loss, or unauthorized access. Sensitive information stored on these devices can be exposed, leading to potential privacy breaches and financial losses.

4. **Unsecured Public Wi-Fi Networks**

Mobile devices often connect to public Wi-Fi networks, which can be unsecured and expose users to man-in-the-middle attacks. Cybercriminals can intercept network traffic and steal sensitive information, such as login credentials and financial data.

5. **Phishing and Social Engineering Attacks**

Mobile devices are increasingly targeted by phishing and social engineering attacks. Users may fall victim to fraudulent emails, SMS messages, or social media posts that trick them into revealing sensitive information or installing malware.

6. **Jailbreaking and Rooting**

Some users may jailbreak (iOS) or root (Android) their devices to gain more control or bypass security restrictions. This compromises the device's built-in security mechanisms and increases the risk of malware installation or unauthorized access to sensitive data.

7. **Bring Your Own Device (BYOD) Challenges**

The trend of employees using personal mobile devices for work purposes introduces additional security challenges. Organizations need to balance security requirements with user privacy and convenience, while ensuring that corporate data is protected on employee-owned devices.

* 1. **Authentication Service Security**

Authentication service security is crucial for protecting mobile devices and networks from various threats. Here are the key aspects of authentication service security:

Security of Devices

* **Mutual Authentication**: Secure network access involves mutual authentication between the device and the base station or web servers to ensure only authenticated devices can connect to the network and access requested services.
* **Typical Attacks on Mobile Devices**: Mobile devices are vulnerable to various attacks through wireless networks, including:
	+ **Denial-of-Service (DoS) attacks**: Overwhelming the device or network with traffic to disrupt services.
	+ **Traffic analysis**: Monitoring network traffic to gather information about the device and its activities.
	+ **Eavesdropping**: Intercepting wireless communications to steal sensitive data.
	+ **Man-in-the-middle attacks**: Inserting an attacker between the device and network to intercept and manipulate communications.

**Security in the Network**

* **Wireless Application Protocol (WAP)**: WAP provides a secure communication layer for mobile devices, ensuring data confidentiality and integrity.
* **Virtual Private Networks (VPN)**: VPNs create an encrypted tunnel between the mobile device and the network, protecting communications from eavesdropping and tampering.
* **MAC Address Filtering**: Restricting network access based on the unique MAC addresses of authorized devices can help prevent unauthorized access.

Additional Security Measures

* **Cryptographic Security**: Using cryptographically generated addresses (CGAs) can enhance the security of mobile devices by providing a way to verify the authenticity of the device's address.
* **LDAP Security**: Securing the Lightweight Directory Access Protocol (LDAP) used for authentication and authorization is crucial to prevent unauthorized access to network resources.
* **RAS Security**: Ensuring the security of Remote Access Services (RAS) used for remote access to corporate networks is essential to prevent unauthorized access and data breaches.

Prevention and Protection Techniques

* **Regular Software Updates**: Keeping mobile devices and network infrastructure up-to-date with the latest security patches helps mitigate known vulnerabilities.
* **Strong Access Controls**: Implementing robust access controls, such as multi-factor authentication and role-based access, can limit unauthorized access to sensitive resources.
* **User Education**: Training users on best practices for mobile device security, such as recognizing phishing attempts and avoiding unsecured Wi-Fi networks, can help reduce the risk of successful attacks.
* **Incident Response Planning**: Having a well-defined incident response plan in place can help organizations quickly detect, contain, and recover from security breaches, minimizing the impact on operations.

**2.10Attacks on Mobile/Cell Phones**

Here are some of the most common attacks on mobile phones:

1. **Malware Attacks**

Mobile malware is a growing threat, with Kaspersky detecting almost 3.5 million pieces of malware on over 1 million user devices in 2014. Malware can steal sensitive data, send premium-rate SMS messages, or even take control of the device.

2. **Phishing Attacks**

Mobile devices are particularly vulnerable to phishing attacks, as users are more likely to open emails and click on links on their phones. Phishing scams often use social engineering tactics to trick users into revealing sensitive information or downloading malware.

3. **Unsecured Wi-Fi Attacks**

Using public Wi-Fi networks can expose mobile devices to various attacks, such as man-in-the-middle attacks and network spoofing. Attackers can set up fake access points to intercept traffic or steal sensitive information.

4. **Smishing (SMS Phishing)**

Smishing is a type of phishing attack that uses SMS messages to trick users into revealing sensitive information or downloading malware. Attackers often pose as legitimate organizations to lure victims.

5. **Bluejacking and Bluesnarfing**

Bluejacking involves sending unsolicited messages to Bluetooth-enabled devices. While relatively harmless, it can be used to send spam or phishing messages. Bluesnarfing is more dangerous, as it exploits Bluetooth vulnerabilities to steal data from devices.

6. **Spyware and Stalkerware**

Spyware and stalkerware are types of malware designed to track a user's location, monitor their activities, and steal sensitive information. These apps are often installed without the user's knowledge or consent.

7. **Replay Attacks**

Replay attacks involve intercepting and retransmitting legitimate network communications to gain unauthorized access or disrupt services. Attackers can use this technique to bypass authentication mechanisms.