1. Cyber Crime Introduction

Cybercrime or a computer-oriented crime is a crime that includes a computer and a network. The computer may have been used in the execution of a crime or it may be the target. Cybercrime is the use of a computer as a weapon for committing crimes such as committing fraud, identity theft, or breaching privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to every field like commerce, entertainment, and government. Cybercrime may endanger a person or a nation's security and financial health. Cybercrime encloses a wide range of activities, but these can generally be divided into two categories:

1. Crimes that aim at computer networks or devices. These types of crimes involve different threats (like virus, bugs etc.) and denial-of-service (DoS) attacks.

2. Crimes that use computer networks to commit other criminal activities. These types of crimes include cyber stalking, financial fraud or identity theft.

Why is Cybercrime considered a grave offense?

There are many privacy concerns surrounding cybercrime when sensitive information is intercepted and leaked to the public, legally or otherwise. Some of that information may include data about military deployments, internal government communications, and even private data about high-value individuals. Cybercrime is not confined to individuals alone. Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation-state is sometimes referred to as cyberwarfare.

In 2018, a study by Center for Strategic and International Studies (CSIS), in partnership with McAfee, a leading cybersecurity firm concludes that close to $600 billion, nearly one percent of global GDP, is lost to cybercrime each year.

Challenges of Cyber Crime:

1. **People are unaware of their cyber rights-**
   The Cybercrime usually happen with illiterate people around the world who are unaware about their cyber rights implemented by the government of that particular country.

2. **Anonymity-**
   Those who Commit cyber crime are **anonymous** for us so we cannot do anything to that person.

3. **Less numbers of case registered-**
   Every country in the world faces the challenge of cyber crime and the rate of cyber crime is increasing day by day because the people who even don't register a case of

cyber crime and this is major challenge for us as well as for authorities as well.

4. **Mostly committed by well educated people-**
   Committing a cyber crime is not a cup of tea for every individual. The person who commits cyber crime is a very **technical** person so he knows how to commit the crime and not get caught by the authorities.

5. **No harsh punishment-**
   In Cyber crime there is no harsh punishment in every cases. But there is harsh punishment in some cases like when somebody commits cyber terrorism in that case there is harsh punishment for that individual. But in other cases there is no harsh punishment so this factor also gives encouragement to that person who commits cyber crime.

Prevention of Cyber Crime:

Below are some points by means of which we can prevent cyber crime:

1. **Use strong password –**
   Maintain different password and username combinations for each account and resist the temptation to write them down. Weak passwords can be easily cracked using certain attacking methods like Brute force attack, Rainbow table attack etc, So make them complex. That means combination of letters, numbers and special characters.

2. **Use trusted antivirus in devices –**
   Always use trustworthy and highly advanced antivirus software in mobile and personal computers. This leads to the prevention of different virus attack on devices.

3. **Keep social media private –**
   Always keep your social media accounts data privacy only to your friends. Also make sure only to make friends who are known to you.

4. **Keep your device software updated –**
   Whenever you get the updates of the system software update it at the same time because sometimes the previous version can be easily attacked.

5. **Use secure network –**
   Public Wi-Fi are vulnerable. Avoid conducting financial or corporate transactions on these networks.

6. **Never open attachments in spam emails –**
   A computer get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know.

7. **Software should be updated –**Operating system should be updated regularly when it comes to internet security. This can become a potential threat when cybercriminals exploit flaws in the system.

Laws against Cybercrime in India

Ever since the introduction of cyber laws in India, the Information Technology Act (IT Act) 2000 covers different types of crimes under cyber law in India. The following types of cybercrimes are covered under the IT Act 2000.

- **Identity theft** – Identity theft is defined as theft of personnel information of an individual to avail financial services or steal the financial assets themselves.
- **Cyberterrorism** – Cyberterrorism is committed with the purpose of causing grievous harm or extortion of any kind subjected towards a person, groups of individuals, or governments.
- **Cyberbullying** – Cyberbullying is the act of intimidating, harassment, defaming, or any other form of mental degradation through the use of electronic means or modes such as social media.
- **Hacking** – Access of information through fraudulent or unethical means is known as hacking. This is the most common form of cybercrime know to the general public.
- **Defamation** – While every individual has his or her right to speech on internet platforms as well, but if their statements cross a line and harm the reputation of any individual or organization, then they can be charged with the Defamation Law.
- **Trade Secrets** – Internet organization spends a lot of their time and money in developing software, applications, and tools and rely on Cyber Laws to protect their data and trade secrets against theft; doing which is a punishable offense.
- **Freedom of Speech** – When it comes to the internet, there is a very thin line between freedom of speech and being a cyber-offender. As freedom of speech enables individuals to speak their mind, cyber law refrains obscenity and crassness over the web.
- **Harassment and Stalking** – Harassment and stalking are prohibited over internet platforms as well. Cyber laws protect the victims and prosecute the offender against this offense.

IT Act, 2000 went through amendments under the Indian Penal Code in the year 2008. These were made in light of the laws on cybercrime – IT Act, 2000 by way of the IT Act, 2008. They were enforced at the beginning of 2009 to strengthen the cybersecurity laws.

Classification of Cyber Crime:

1. **Cyber Terrorism –**
   Cyber terrorism is the use of the computer and internet to perform violent acts that result in loss of life. This may include different type of activities either by software or hardware for threatening life of citizens.
   In general, Cyber terrorism can be defined as an act of terrorism committed through the use of cyberspace or computer resources.

2. **Cyber Extortion –**
   Cyber extortion occurs when a website, e-mail server or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers.

These hackers demand huge money in return for assurance to stop the attacks and to offer protection.

3. **Cyber Warfare –**
   Cyber warfare is the use or targeting in a battle space or warfare context of computers, online control systems and networks. It involves both offensive and defensive operations concerning to the threat of cyber attacks, espionage and sabotage.

4. **Internet Fraud –**
   Internet fraud is a type of fraud or deceit which makes use of the Internet and could include hiding of information or providing incorrect information for the purpose of deceiving victims for money or property. Internet fraud is not considered a single, distinctive crime but covers a range of illegal and illicit actions that are committed in cyberspace.

5. **Cyber Stalking –**
   This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. In this case, these stalkers know their victims and instead of offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

6. **Phishing**
   It is a process of acquiring personal and sensitive information of an individual via email by disguising as a trustworthy entity in an electronic communication. The purpose of phishing is identity theft and the personal information like username, password, and credit card number etc. may be used to steal money from user account. If a telephone is used as a medium for identity theft, it is known as Vishing (voice phishing). Another form of phishing is Smishing, in which sms is used to lure customers.

7. **Forgery and Counterfeiting**
   It is a use of computer to forgery and counterfeiting is a document. With the advancement in the hardware and the software, it is possible to produce counterfeit which matches the original document to such an extent that it is not possible to judge the authenticity of the document without expert judgement.

8. **Child Pornography**
   It is an act of possessing image or video of a minor (under 18), engaged in sexual conduct.

9. **Software Piracy and Crime related to IPRs**
   Software piracy is an illegal reproduction and distribution for personal use or business. It comes under crime related to IPR infringement. Some of the other crimes under IPR infringement are: downloading of pirated software, songs, movies, etc.

Hacking

In the context of computer security, hacking refers to the unauthorized access, manipulation, or exploitation of computer systems or networks. This can include activities such as breaking into a computer system, stealing sensitive information, or disrupting normal system functions. Hacking, when used to gain unauthorized access to computer systems, networks, or data, is a criminal activity. Perpetrators, known as hackers, exploit vulnerabilities to steal sensitive information, disrupt services, or commit fraud. Such actions violate privacy, compromise security, and can lead to severe legal consequences, including fines and imprisonment. Cybersecurity measures are crucial to prevent and mitigate the impact of hacking crimes in an increasingly digital world.

Types of Hackers

Grey, black, and white hackers are terms used to categorize individuals based on their ethical and moral stance when it comes to hacking and cybersecurity. These terms help differentiate between hackers who use their skills for different purposes. Here's an overview of each type:

1. **White Hat Hacker**:
    - **Ethical Intentions**: White hat hackers, also known as ethical hackers, are individuals who use their hacking skills for good and with ethical intentions.
    - **Legal**: They operate within the boundaries of the law and typically have permission to test and secure computer systems, networks, and software.
    - **Goals**: Their primary goal is to identify and fix vulnerabilities and weaknesses in computer systems and network infrastructure to strengthen security.
    - **Examples**: White hat hackers may work as security professionals, penetration testers, or cybersecurity consultants.

2. **Grey Hat Hacker**:
    - **Ambiguous Intentions**: Grey hat hackers are somewhere in between white and black hat hackers. They may have mixed motivations, and their actions can be morally ambiguous.
    - **Legal**: They may perform hacking activities without explicit authorization, which can be illegal in some cases.
    - **Goals**: Grey hat hackers may identify vulnerabilities and disclose them to the affected parties without consent, sometimes with the expectation of receiving a reward or acknowledgment.
    - **Examples**: Some grey hat hackers disclose security flaws they discover, but they may not always follow legal procedures or ethical guidelines.

3. **Black Hat Hacker**:
    - **Malicious Intentions**: Black hat hackers are individuals who engage in hacking with malicious intent. Their actions are typically illegal and unethical.
    - **Illegal**: They break into computer systems, networks, and software without permission and often for personal gain or to cause harm.

- **Goals**: Their primary goals include stealing data, spreading malware, conducting cyberattacks, and engaging in criminal activities.
- **Examples**: Cybercriminals, hackers involved in identity theft, data breaches, and other illicit activities fall into this category.

Phases of Hacking

Hacking typically involves several phases, often referred to as the "hacking lifecycle" or "cyberattack lifecycle." These phases may vary slightly depending on the model or framework being used, but generally include the following:

1. **Reconnaissance (Information Gathering):** In this phase, hackers gather information about the target, such as identifying potential vulnerabilities, system architecture, and the network environment. This can involve passive methods, like searching for publicly available information, or active methods, such as network scanning.
2. **Scanning:** Hackers use various tools and techniques to actively scan the target network for open ports, services, and vulnerabilities. This phase helps them identify potential entry points into the system.
3. **Gaining Access (Exploitation):** Once vulnerabilities are identified, hackers attempt to exploit them to gain unauthorized access to the target system. This may involve using known exploits, social engineering, or other methods to compromise security.
4. **Maintaining Access:** After successfully gaining access, hackers aim to maintain a persistent presence in the system. This involves installing backdoors, rootkits, or other means to ensure continued access, even if the initial point of entry is discovered and addressed.
5. **Covering Tracks:** To avoid detection, hackers cover their tracks by deleting logs, modifying timestamps, and taking other actions to erase evidence of their activities. This makes it more difficult for security professionals to trace the attack back to its source.