Cyber Crime

Cyber crime or 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.  
Cyber crime is the use of a computer as a weapon for committing crimes such as committing fraud, identities theft or breaching privacy. Cyber crime, especially through the Internet, has grown in importance as the computer has become central to every field like commerce, entertainment and government. Cyber crime may endanger a person or a nation’s security and financial health.

Cyber crime encloses a wide range of activities but these can generally be divided into two categories:

1. Crimes that aim computer networks or devices. These types of crimes involves 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.

**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 ,

**Cyberwarfare** refers to the use of digital attacks -- like computer viruses and hacking -- by one country to disrupt the vital computer systems of another, with the aim of creating damage, death and destruction.

**4.Internet Fraud:**  
Internet fraud is a type of fraud 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.

The most common types of online fraud are called **phishing** and spoofing. **Phishing** is the process of collecting your personal information through e-mails or websites claiming to be legitimate. This information can include usernames, passwords, credit card numbers, social security numbers, etc.

**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.

**Types of Cyber Stalking:**

* **Webcam Hijacking:**  
  Internet stalkers would attempt to trick you into downloading and putting in a malware-infected file that may grant them access to your webcam. the method is therefore that it’s probably you wouldn’t suspect anything strange.
* **Observing location check-ins on social media:**  
  In case you’re adding location check-ins to your Facebook posts, you’re making it overly simple for an internet stalker to follow you by just looking through your social media profiles.
* **Catfishing:**  
  Catfishing happens via social media sites, for example, Facebook, when internet stalkers make counterfeit user-profiles and approach their victims as a companion of a companion.

Catfishing is a deceptive activity where a person creates a sockpuppet presence or fake identity on a social networking service, usually targeting a specific victim for abuse or fraud. Catfishing is often employed for romance scams on dating website.

**6.Identity Theft** also called Identity Fraud is a crime which is being committed in a huge number nowadays. Using the identity of another person and attempting a practice for personal profit is termed as Identity threat.

This theft is committed in many ways by gathering personal information such as transactional information of another person to make transactions.

**Example –**  
 Thieves use different mechanisms to extract information of customer’s credit cards from the corporate databases, once they are aware of the information they can easily degrade the rating of the victim’s credit card.

Having this information with the thieves can make you cause huge harm if not notified earlier. With these false credentials, they can obtain a credit card in the name of the victim which can be used for covering false debts.

**7.Credit card account theft**

**Credit card** fraud happens when someone — a fraudster or a thief — uses your stolen **credit card** or the information from that **card** to make unauthorized purchases in your name or take out cash advances using your account. **Credit card** fraud isn't rare, and it could happen to you.

**8.Copyright infringement**

* Copyright infringement is the use of works protected by copyright law without permission for a usage where such permission is required, thereby infringing certain exclusive rights granted to the copyright .
* **Examples**
* :
* Downloading movies and music without proper payment for use.
* Recording movies in a theater.
* Using others' photographs for a blog without permission.
* Copying software code without giving proper credit.
* Creating videos with unlicensed music clips.

**9.Child pornography**

**10.spreding malwareslikes virus,worms,Trojan horse**

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