## → What is cyber crime?

Cyber crime is a crime committed in cyber world, which involves use of computers, Internet and other IT tools and technologies. There are cyber laws defined by the government. Any offensive activity conducted using internet and computers that matches the definition of crime in the book of cyber laws is called cyber crime and is punishable by law.

Cybercrime is defined as a crime where a computer is the object of the crime or is used as a tool to commit an offense. A cybercriminal may use a device to access a user's personal information, confidential business information, government information, or disable a device. It is also a cybercrime to sell or elicit the above information online.

Cyber crime is a broad term that is used to define criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It also covers the traditional crimes in which computers or networks are used to enable the illicit activity.

**Categories of Cybercrime**

**1. Crimes against People**

These crimes include cyber harassment and stalking, distribution of child pornography, credit card fraud, human trafficking, spoofing, identity theft.

**2. Crimes against Property**

Some online crimes occur against property, such as a computer or server. These crimes include DDOS attacks, hacking, virus transmission, cyber and typo squatting, computer vandalism, copyright infringement, and IPR violations.

**3. Crimes against Government**

When a cybercrime is committed against the government, it is considered an attack on that nation's sovereignty. Cybercrimes against the government include hacking, accessing confidential information, cyber warfare, cyber terrorism, and pirated software.

# Different types of cyber crimes

## → Unauthorized Access and Hacking

Unauthorized access means any kind of access without the permission of either of the rightful or person in charge of the computer, computer system or computer network. Hacking means an illegal intrusion into a computer system and/or network. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. Government websites are the most targeted sites for the hackers.

## → Trojan, Virus and Worm Attacks

**What is a Trojan horse?**

A Trojan horse is a program that allows the attack to control the user's computer from a remote location. The program is usually disguised as something that is useful to the user. Once the user has installed the program, it has the ability to install malicious payloads, create backdoors, install other unwanted applications that can be used to compromise the user's computer, etc.

Activities that the attacker can perform using a Trojan horse:

- Use the user's computer as part of the Botnet when performing distributed denial of service attacks.
- Damage the user's computer (crashing, blue screen of death, etc.)
- Stealing sensitive data such as stored passwords, credit card information, etc.
- Modifying files on the user's computer
- Electronic money theft by performing unauthorized money transfer transactions
- Log all the keys that a user presses on the keyboard and sending the data to the attacker. This method is used to harvest user ids, passwords, and other sensitive data.
- Viewing the users' screenshot
- Downloading browsing history data

**What is a Virus?**

A virus is a computer program that attaches itself to legitimate programs and files without the user's consent. Viruses can consume computer resources such as memory and CPU time. The attacked programs and files are said to be "infected".

A computer virus may be used to:

- Access private data such as user id and passwords
- Display annoying messages to the user
- Corrupt data in your computer
- Log the user's keystrokes

Computer viruses have been known to employ social engineering techniques. These techniques involve deceiving the users to open the files which appear to be normal files such as Word or Excel documents. Once the file is opened, the virus code is executed and does what it's intended to do.

**What is a worm?**

A worm is a malicious computer program that replicates itself usually over a computer network. An attacker may use a worm to accomplish the following tasks;

Install backdoors on the victim's computers. The created backdoor may be used to create zombie computers that are used to send spam emails, perform distributed denial of service attacks, etc. the backdoors can also be exploited by other malware.

Worms may also slowdown the network by consuming the bandwidth as they replicate.

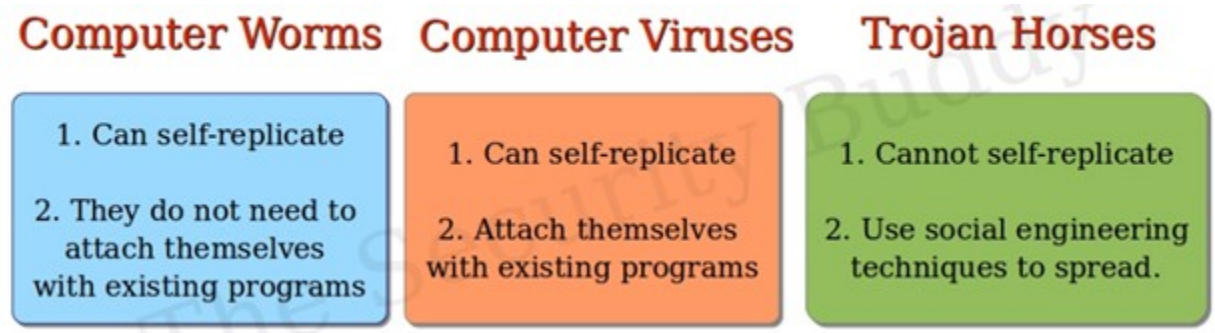
Install harmful payload code carried within the worm.

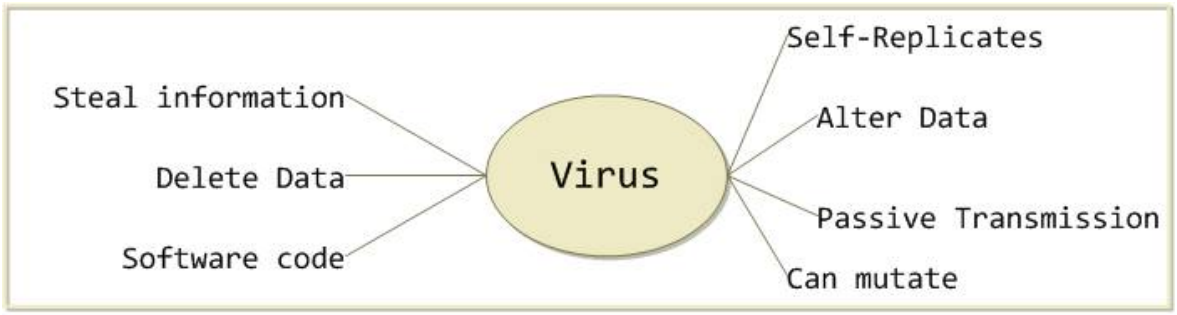
**Trojans, Viruses, and Worms counter measures**

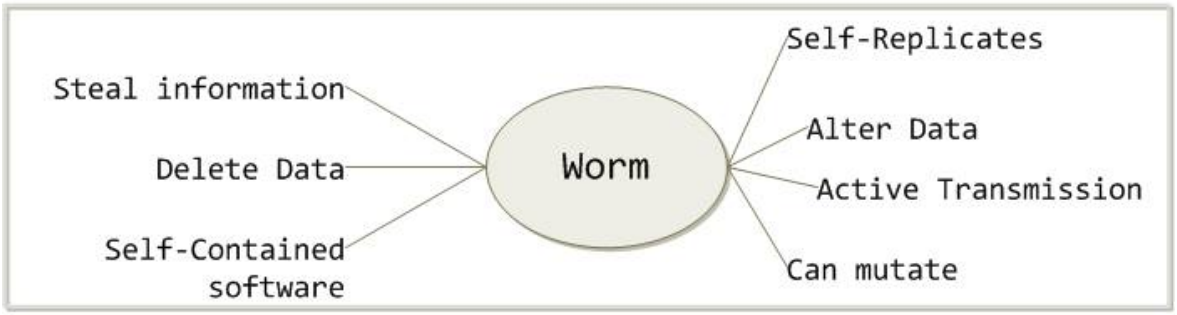
To protect against such attacks, an organization can use the following methods.

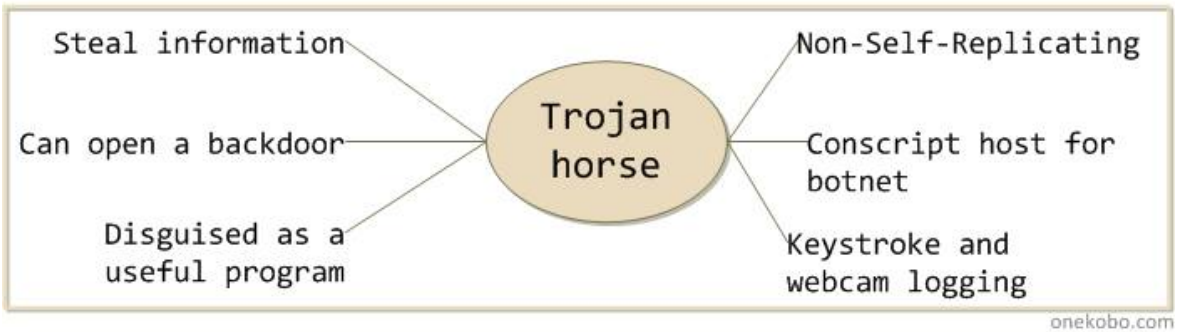
- A policy that prohibits users from downloading unnecessary files from the Internet such as spam email attachments, games, programs that claim to speed up downloads, etc.
- Anti-virus software must be installed on all user computers. The anti-virus software should be updated frequently, and scans must be performed at specified time intervals.
- Scan external storage devices on an isolated machine especially those that originate from outside the organization.

- Regular backups of critical data must be made and stored on preferably read-only media such as CDs and DVDs.
- Worms exploit vulnerabilities in the operating systems. Downloading operating system updates can help reduce the infection and replication of worms.
- Worms can also be avoided by scanning all email attachments before downloading them.



## → E-mail related crimes

**E-mail spoofing**

- Email spoofing refers to email that appears to originate from one source but actually has been sent from another source. Email spoofing can also cause monetary damage.
- E-mail spoofing is e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. Because core SMTP doesn't provide any authentication, it is easy to impersonate and forge emails.
- Because the purpose is so often malicious, "spoof" (an expression whose base meaning is innocent parody) is a poor term for this activity which can confuse newcomers to it, so that more accountable organizations such as government departments and banks tend to avoid it, preferring more explicit descriptors such as "fraudulent" or "phishing.

**Email Spamming**

Email spam, also known as junk email or unsolicited bulk email (UBE), is a subset of spam that involves nearly identical messages sent to numerous recipients by email. Email spam has steadily grown since the early 1990s. Botnets, networks of virus-infected computers, are used to send about 80% of spam. Spammers collect email addresses from chatrooms, websites, customer lists, newsgroups, and viruses which harvest users' address books, and are sold to other spammers. They also use a practice known as "email appending" or "epending" in which they use known information about their target (such as a postal address) to search for the target's email address. Much of spam is sent to invalid email addresses. Spam averages 78% of all email sent. According to the Message Anti-Abuse Working Group, the amount of spam email was between 88–92% of email messages sent in the first half of 2010.

**Email Bombing**

An e-mail bomb is a form of net abuse consisting of sending huge volumes of e-mail to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack.

**Email Threatening**

Email is a useful tool for technology savvy criminals thanks to the relative anonymity offered by it. It becomes fairly easy for anyone with even a basic knowledge of computers to become a blackmailer by threatening someone via e-mail.

## → Denial-of-Service (DoS) attack

It is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

There are two general methods of DoS attacks: **flooding services or crashing services**. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop.

**Buffer overflow attacks** – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks.

**ICMP flood** – leverages mis-configured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.

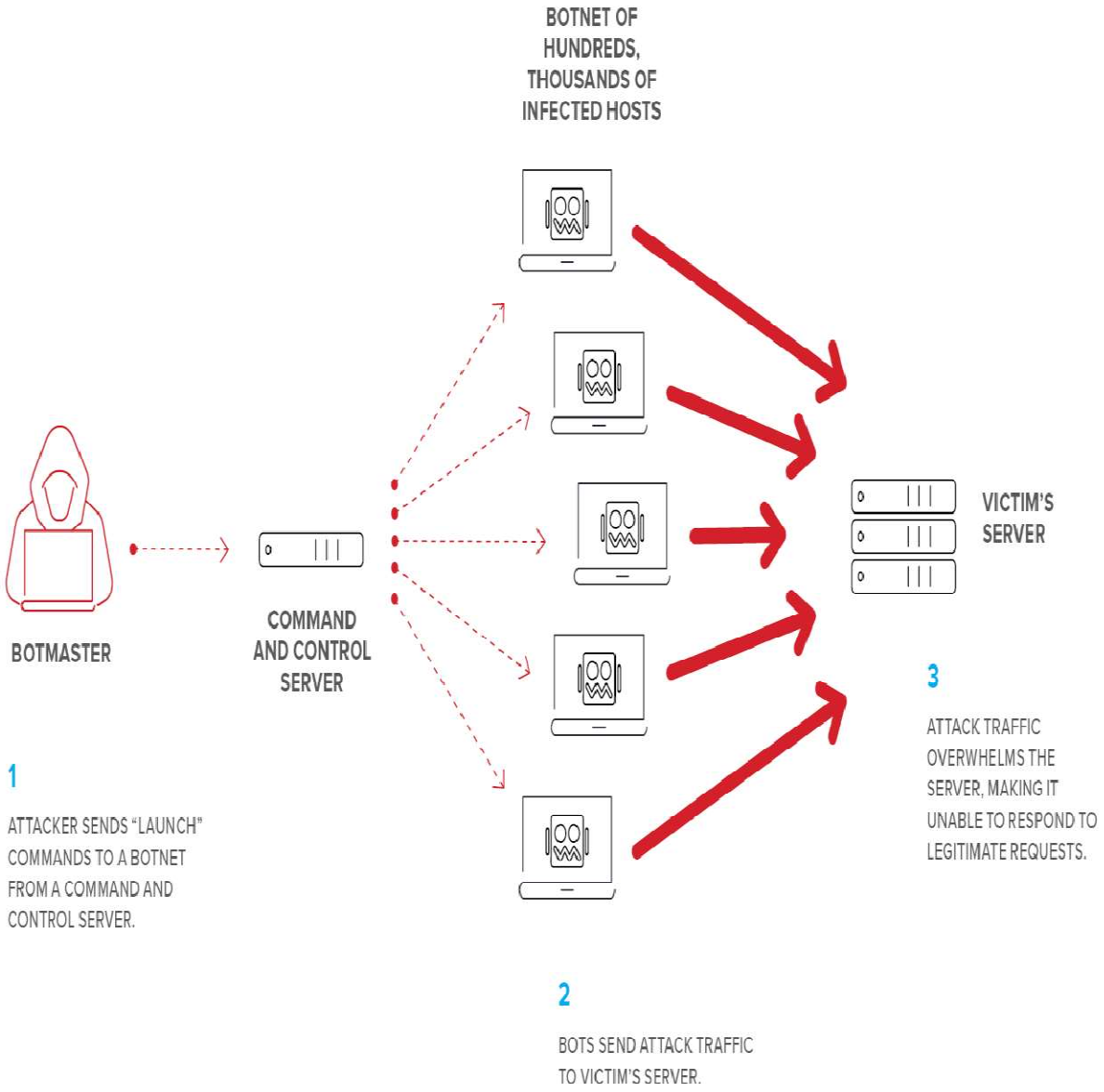
**SYN flood** – sends a request to connect to a server, but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

**Distributed Denial of Service (DDoS) attack:**

A DDoS attack occurs when multiple systems orchestrate a synchronized DoS attack to a single target. The essential difference is that instead of being attacked from one location, the target is attacked from many locations at once. The distribution of hosts that defines a DDoS provide the attacker multiple advantages:

- He can leverage(use something to maximum advantage) the greater volume of machine to execute a seriously disruptive(causing troublemaking) attack.
- The location of the attack is difficult to detect due to the random distribution of attacking systems (often worldwide)

- It is more difficult to shut down multiple machines than one.
- The true attacking party is very difficult to identify, as they are disguised behind many (mostly compromised) systems.



## → IPR Violations

Intellectual property (IP) is a category of property that includes intangible creations of the human intellect. There are many types of intellectual property, and some countries recognize more than others. The best-known types are patents, copyrights, trademarks, and trade secrets.

An intellectual property (IP) infringement (violation) is the infringement or violation of an intellectual property right. There are several types of intellectual property rights, such as copyrights, patents, trademarks, industrial designs, and trade secrets. These kind of crimes also include copyright infringement, trademarks violations, theft of computer source code, patent violations etc. Domain names are also trademarks and protected by ICANN's domain dispute resolution policy and also under trademark laws. Cyber squatters register domain name identical to popular service provider's name so as to attract their users and get benefit from them.

Therefore, an intellectual property infringement may for instance be one of the following:

- Copyright infringement, for example a software copyright infringement
- Patent infringement
- Trademark infringement
- Design infringement
- Cyber squatting

**Software Piracy:** Software piracy refers to the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.

## → Cyber squatting (domain squatting)

Cybersquatting refers to illegal domain name registration or use. Cybersquatting can have a few different variations, but its primary purpose is to steal or misspell a domain name in order to profit from an increase in website visits, which otherwise would not be possible.

Trademark or copyright holders may neglect to reregister their domain names, and by forgetting this important update, cybersquatters can easily steal domain names. Cybersquatting also includes advertisers who mimic domain names that are similar to popular, highly trafficked websites.

Cybersquatting registrants obtain and use the domain name with the bad faith intent to profit from the goodwill of the actual trademark owner.

The Internet Corporation for Assigned Names and Numbers (ICANN) is a nonprofit organization charged with overseeing domain name registration.

At the moment, the four most common types of cybersquatting are;

1. Typosquatting
2. identity theft
3. name jacking
4. reverse-cybersquatting

**Typosquatting**

Typosquatting (a.k.a URL hijacking) targets Internet users who enter a website address incorrectly into their browser. For example, typing “Gooogle.com” instead of “Google.com.”

**Identity theft**

Identity theft describes crimes where someone unlawfully obtains and uses another individual’s private data to involve deception or fraud, usually for financial gain. cybersquatters may buy a domain that was inadvertently not renewed by the previous owner. Cybersquatters use specialized software applications to easily monitor the expiration dates of targeted domain names. After registering expired domain names, cybersquatters may link them to websites duplicates of the previous domain name owners’ websites. As a result, cybersquatters will track visitors to their websites into thinking they are visiting the websites of the last name domain owners.

**Name jacking**

The registration of a domain name associated with an individual’s name, usually a celebrity or a well-known public figure, is referred to as name jacking. Name jackers profit from web traffic related to the individuals being targeted.

For example, Tom Cruise took his case to the WIPO in 2006 against Jeff Burgar, who had owned the domain TomCruise.com for over ten years. Users were redirected to his website Celebrity1000.com, which earns money through third-party advertisements.

**Reverse-cybersquatting**

Reverse-cybersquatting is an aggressive action that a cybersquatter uses to obtain a specific domain name on the Internet. Cybersquatters may use intimidation and pressure to transfer legitimate ownership of a domain name to the person or organization that owns a registered trademark reflected in the domain name.

## → Cyber smearing (defamation)

Defamation is injury to the reputation of a person. Cyber defamation occurs when defamation takes place with the help of computers and / or the Internet.

When a person publishes defamatory matter about someone on a website, social media or sends e-mails containing defamatory information to all of that person's friends, it is termed as cyber defamation (the action of damaging the good reputation of someone).

The three essentials of defamation are:

- The statement must be false and defamatory,
- The said statement must refer to the victim, and
- The statement must be published.

A person's reputation is his or her property and sometimes even more valuable than physical property. Cyber criminals may also disclose victims' personal data (e.g. real name, address, or workplace/ schools) on various immoral websites.

Cases of piggy-backing (ink to or take advantage of) on victim's identity are now common. This could be used to publish objectionable material in their name that defames or ridicules a person.

## → Cyber stalking

In general terms, stalking can be termed as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing(deliberate destruction) victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim. Cyber Stalking means repeated acts of harassment or threatening behavior of the cyber criminal towards the victim by using internet services. Both kind of Stalkers i.e., Online & Offline – have desire to control the victims life.

Some examples of cyber stalking practice are:

- They collect all personal information about the victim such as name, family background, Telephone Numbers of residence and work place, daily routine of the victim, address of residence and place of work, date of birth etc. If the stalker is one of the acquaintances of the victim he can easily get this information. If stalker is a stranger to victim, he collects the information from the internet resources such as various profiles, the victim

may have filled in while opening the chat or e-mail account or while signing an account with some website.

- The stalker may post this information on any website related to sex-services or dating services, posing as if the victim is posting this information and invite the people to call the victim on her telephone numbers to have sexual services. Stalker even uses very filthy and obscene language to invite the interested persons.
- People of all kind from nook and corner of the World, who come across this information, start calling the victim at her residence and/or work place, asking for sexual services or relationships.
- Some stalkers subscribe the e-mail account of the victim to innumerable pornographic and sex sites, because of which victim starts receiving such kind of unsolicited e-mails.
- Some stalkers keep on sending repeated e-mails asking for various kinds of favors or threaten the victim.
- In online stalking the stalker can make third party to harass the victim.
- Follow their victim from board to board. They "hangout" on the same BB's as their victim, many times posting notes to the victim, making sure the victim is aware that he/she is being followed. Many times they will "flame" their victim (becoming argumentative, insulting) to get their attention.
- Stalkers will almost always make contact with their victims through email. The letters may be loving, threatening, or sexually explicit. He will many times use multiple names when contacting the victim.

## → Financial crimes (banking, credit/debit card related)

Financial cybercrime includes activities such as stealing payment card information, gaining access to financial accounts in order to initiate unauthorised transactions, extortion, identity fraud in order to apply for financial products, and so on.

Some examples are:

- An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities.
- Merchandise or services that were purchased or contracted by individuals online are never delivered.
- The non-delivery of products purchased through an Internet auction site.
- Investors are enticed to invest in fraudulent scheme by the promises of abnormally high profits.

Top 5 cybercrimes affecting businesses and individuals:

- Phishing Scams.
- Website Spoofing.
- Ransomware.
- Malware.
- IOT Hacking.

Cyber Crime In Banking Industry means digital misconduct where the criminal exercises a number of wrongdoings such as money transfers and withdrawals via unauthorized access by using the computer or any other electronic devices and the internet.

Identity thieves can retrieve account data from your card's magnetic strip using a device called a skimmer, which they can stash in ATMs and store card readers. They can then use that data to produce counterfeit cards.

Sophisticated techniques, enable criminals to produce fake and doctored cards. Then there are also those who use skimming to commit fraud. Skimming is where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another.

## → Other types of cyber crimes

**Web Hijacking**

Web hijacking means taking forceful control of another person's website. In this case the owner of the website loses control over his website and its content.

**Pornography**

Pornography means showing sexual acts in order to cause sexual excitement. The definition of pornography also includes pornographic websites, pornographic magazines produced using computer and the internet pornography delivered over mobile phones.

**Child Pornography**

The Internet is being highly used as a medium to sexually abuse children. The children are viable victim to the cyber crime. Computers and internet having become a necessity of every household, the children have got an easy access to the internet. There is an easy access to the pornographic contents on the internet. Pedophiles lure the children by distributing pornographic material and then they try to meet them for sex or to take their nude photographs including their engagement in sexual positions. Sometimes Pedophiles contact

children in the chat rooms posing as teenagers or a child of similar age and then they start becoming friendlier with them and win their confidence. Then slowly pedophiles start sexual chat to help children shed their inhibitions about sex and then call them out for personal interaction. Then starts actual exploitation of the children by offering them some money or falsely promising them good opportunities in life. The pedophiles then sexually exploit the children either by using them as sexual objects or by taking their pornographic pictures in order to sell those over the internet.

**Salami attacks**

These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 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 of money every month.

**Phishing**

Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information. By spamming large groups of people, the phisher counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with legitimately.

**Sale of illegal articles**

This category of cyber crimes includes sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.

**Online gambling**

There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering. Cases of transactions and money laundering over the Internet have been reported.

**Email spoofing**

Email spoofing refers to email that appears to originate from one source but actually has been sent from another source. Email spoofing can also cause monetary damage.

**Cyber Defamation**

When a person publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends, it is termed as cyber defamation (the action of damaging the good reputation of someone).

**Forgery**

The action of forging a copy or imitation of a document, signature. Computers, printers and scanners are used to forge counterfeit currency notes, postage and revenue stamps, mark sheets etc. These are made using computers, and high quality scanners and printers.

**Cyber Terrorism**

Cyber terrorism is a cyber crime against country and its government and military. Cyber terrorism targeted attacks are on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc.

Cyber terrorism is an attractive option for modern terrorists for several reasons;

- It is cheaper than traditional terrorist methods.
- Cyber terrorism is more anonymous than traditional terrorist methods.
- The variety and number of targets are enormous.
- Cyber terrorism can be conducted remotely, a feature that is especially appealing to terrorists.
- Cyber terrorism has the potential to affect directly a larger number of people