The common types of cybercrimes are: -

Hacking – An unauthorized user who attempts to or gains access to an information system is known as hacker. Hacking is a cybercrime even if there is no visible damage to the system, because it is an invasion in to the privacy of data.

There are 3 different classes of Hackers.

White Hat Hackers – They are those hackers who believe that information sharing is good, and that it is their duty to share their expertise by facilitating access to information. However, there are some white hat hackers who are just "joy riding" on computer systems.

Black Hat Hackers – Black hat hackers cause damage after intrusion. They may steal or modify data or insert viruses or worms which damage the system. They are also known as crackers.

Grey Hat Hackers – These types of hackers are typically ethical but occasionally they can violate the hacker ethics. They will hack into networks, stand-alone computers and software. Network hackers try to gain unauthorized access to private computer networks just for challenge, curiosity, and distribution of information.

Cyber Stalking – Cyber stalking involves use of internet to harass someone. The behavior includes false accusations, threats etc. Normally, majority of cyber stalkers are men and the majority of victims are women.

Spamming – Spamming is sending of unsolicited bulk and commercial messages over the internet. Although irritating to most email users, it is not illegal unless it causes damage such as overloading network and disrupting service to subscribers or creates negative impact on consumer attitudes towards Internet Service Provider.

Cyber Pornography – With the increasing approach of internet to the people, there is also an increase in the victimization of Women and children for sexual exploitation through internet

Cyber Phishing – It is a criminally fraudulent process in which cyber-criminal acquires sensitive information such as username, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.

Software Piracy – It is an illegal reproduction and for business or personal use. This is considered to be a type of infringement of copy right and a violation of a license agreement. Since for unauthorized user is not a party to the license agreement it is difficult to find out remedies. There are numerous cases of software piracy. Infact according to one report New Delhi's Nehru market is the Asia's largest market where one can easily find pirated software.

Money Laundering – Money laundering basically means the moving of illegally acquired cash through financial and other systems so that it appears to be legally acquired. This is possible prior to computer and internet technology and now times electronic transfers have made it easier and more successful.

Password Sniffers – These are programs that monitor and record the name and password of network users as they log in, jeopardizing security at a site. Whoever installs the sniffer can impersonate an authorized user and log in to access on restricted documents.

Spoofing – "poofing is the act of disguising one computer to electronically "look" like another compute, in order to gain access to a system that would be normally is restricted.

Credit Card Fraud – In U.S.A. half a billion dollars have been lost annually by consumers who have credit cards and calling card numbers. These are stolen from on-line databases. In present world this cybercrime is emerged as a major threat as numerous cases had been filed in almost every major developed and developing country.

Web Jacking – The term refers to forceful taking of control of a web site by cracking the password.

Cyber terrorism – The use of computer resources to intimidate or coerce government, the civilian population or any segment thereof in furtherance of political or social objectives is called cyber terrorism. Individuals and groups quite often try to exploit anonymous character of the internet to threaten governments and terrorize the citizens of the country

Cyber defamation is not a specific criminal offense, misdemeanor or tort, but rather defamation or slander conducted via digital media, usually through the Internet.

Penalties for "cyber defamation" vary from country to country, but the fundamental rights covered in the UN Declaration of Human Rights and European Union Fundamental Human Rights.

Stopping or addressing defamation can be difficult. If the person has no serious grudge, then a cease and desist letter may stop the behavior and get the statements removed from the Internet. On the other hand, if the person is acting out of spite, it may be necessary to file a report with the police depending on local law.

Pharming is a cyber-attack intended to redirect a website's traffic to another, fake site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real IP addresses. Compromised DNS servers are sometimes referred to as "poisoned". Pharming requires unprotected access to target a computer, such as altering a customer's home computer, rather than a corporate business server.

Firewall

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet. A firewall can be hardware, software, or both.

Packet filtering: The system examines each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

Circuit-level gateway implementation: This process applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

Acting as a proxy server: A proxy server is a type of gateway that hides the true network address of the computer(s) connecting through it. A proxy server connects to the Internet, makes the requests for pages, connections to servers, etc., and receives the data on behalf of the computer(s) behind it.

Web application firewall: A web application firewall is a hardware appliance, server plug-in, or some other software filter that applies a set of rules to a HTTP conversation. Such rules are generally customized to the application so that many attacks can be identified and blocked.

Computer Ethics & Good Practices: -

Ethics deals with placing a "value" on acts according to whether they are "good" or "bad". Every society has its rules about whether certain acts are ethical or not. These rules have been established because of consensus in society and are often written into laws.

The Ten Commandments of computer ethics have been defined by the Computer Ethics Institute. Here is our interpretation of them:

Do not use a computer to harm other people: If it is unethical to harm people by making a bomb, for example, it is equally bad to write a program that handles the timing of the bomb. Or, to put it more simply, if it is bad to steal and destroy other people's books and notebooks, it is equally bad to access and destroy their files

Do not interfere with other people's computer work: Computer viruses are small programs that disrupt other people's computer work by destroying their files, taking huge amounts of computer time or memory, or by simply displaying annoying messages. Generating and consciously spreading computer viruses are unethical.

Do not snoop around in other people's files: 'eading other people's e-mail messages are as bad as opening and reading their letters: This is invading their privacy. Obtaining other people's non-public files should be judged the same way as breaking into their rooms and stealing their documents. Text documents on the Internet may be protected by encryption.

Do not use a computer to steal: Using a computer to break into the accounts of a company or a bank and transferring money should be judged the same way as robbery. It is illegal and there are strict laws against it.

Do not use a computer to bear false witness: The Internet can spread untruth as fast as it can spread the truth. Putting out false "information" to the world is bad. For instance, spreading false rumors about a person or false propaganda about historical events is wrong.

Do not use or copy software for which you have not paid: Software is an intellectual product. In that way, it is like a book: Obtaining illegal copies of copyrighted software is as bad as photocopying a copyrighted book. There are laws against both. Information about the copyright owner can be embedded by a process called watermarking into pictures in the digital format.