**Computer Security Threats :**

The accelerated development of Internet technologies has facilitated our everyday activities like surfing the Internet to obtain information, to connect with colleagues around the world, to look for better job opportunities, to explore new places and the like. These pieces of information are made available, whether free or not, due to the Internet network. However, we should be aware of the possible threats that are lurking on the world wide web when online. cybercriminals often find a gap in our computer security system. They target these vulnerabilities to conduct an exploit- based attack through designing malicious software programs to attack our computers especially those of celebrities, politicians, big companies, etc. there are several types of computer security threats such as viruses, Trojans, spam, worms, spyware, denial of service attacks, botnet, etc.

1. **Virus:**

It is a malicious software program that attach itself covertly to downloads and performs malicious actions. It is shared through CDs, DVDs, USB sticks, or loaded on to computers by opening infected email attachment. A computer virus can destruct the files or the system.

1. **Trojan horse:**

It is a program that is not inserted without the knowledge of the user. It has a remote control .i.e. computers infected by a Trojan are completely under the control of the haker. Once a Trojan horse embedded application is downloaded in your computer , a Trojan horse can do anything from recording your confidential information to hijacking your web cameras to watch and record your whole movement in business.

1. **Spam:**

Spam is messages sent to somebody containing unrelated information during Internet activity. The purpose of spam is to advertise certain products or services. These ads are usually inserted by viruses, trojans, or worms. Spam is very harmful to organizations that use email facilities primarily for military and state activities. Spam can cause stacks on useless messages. It will be fatal. The operating system will not be able to withstand the amount of spam sent to the system. Spam also often contains malware so that the system will send spam to other computers while connected to the Internet.

1. **Worms:**

A worm is a computer program that can perform self-duplication on a system. It usually makes its way on to a computer through a malicious email attachment or USB stick. Once your computer has been infected by a worm, it will likely send itself to every email address logged in your system. To the receiver, your email will appear harmless, until they open it and get infected by the same worm.

1. **Spyware:**

Spyware is a program that can record secretly any computer network activity. It can steal PIN, password, bank account and others. The recorded data will be sent to the virus maker. If there is valuable data, it will be sold to other parties who can drop the opponent. Spyware deployment cannot be detected. It comes from programs that are downloaded from the internet that is usually already modified and inserted by spyware programs. Spyware can degrade and damage the performance of the operating system and application programs installed on the computer. It is a program that is difficult to be discarded even though the computer is already doing the recovery process

1. **Denial of Service Attacks:**

 A distributed denial of service attacks occurs when a malicious user gets a network of zombie computers to sabotage a particular web or server. The attack occurs when the malicious user tells all zombie computers to link with specific site or server frequently that increases the volume of traffic overloads and results with the shutdown of that website or server.

1. **Botnet:**

A botnet is a group of computers or software robots or bots that perform repetitive tasks over the Internet. Malicious bots are programs designed to secretly install themselves on vulnerable computers. It creates a battalion of infected computers known as zombies when get connected to the Internet by the originator. The originator remotely controls them. It can spread all types of malware, send spam with viruses attached, use one computer to infect others, etc.

Cybercriminals use various types of viruses to breach the security of our computers, they install a Trojan horse for creating backdoor to discover our confidential information. Send spam with viruses attached and the like.