TROJANS & WORMS

Trojans and warms are two different kinds of malicious software that can cause same type of damage. Let us elaborate,

Trojans:

Trojans are one kind of malware which was named after Greek name Trojan horses. They look legitimate and trick the used to loaf and execute them on their system. After the user executes them, they can cause numerous effects ranging from annoying popup to destroying the functions and damaging the host. They have the capability of creating a back door for the host system and increase the chances of compromising personal and confidential information. Unlike worms, they don't reproduce by replicating or infecting other files. Some of the notable Trojans are net bus, beast, Zeus etc., some of the Trojans may gain access to system's inter connections, email and passwords. They may even interrupt emails. These Trojans are so dangerous that they can provide remote access of the host's hard drive to some other person/hacker who can keep track of your data.

Worms:

Worms can cause similar type of damages as a virus, but the only difference is unlike virus which requires spreading of infected file, Worms are stand alone software which exploits vulnerabilities on the target systems or uses some methods to trick the users into executing them. The main capacity of a worm that makes it so dangerous is its ability to replicate itself. Instead of sending a single worm out, it can send hundreds and hundreds of worms which can create a huge effect.

We can remove these Trojans and worms automatically or manually. We can use antivirus programs to deal with these malicious software or we can remove them manually. Download the auto runs from sys internals and reboot the system in safe

Install all anti-viruses, and ensure that they are kept up to date. New viruses can spread very quickly, so have an updated infrastructure in place that can update all the computers in your company seamlessly, frequently, and at short notice.

You also need to run email filtering software at your email gateway as well, in order to protect your business from the threats of email-borne viruses, spam and spyware. And don't forget to protect your laptop computers and desktop computers used by home workers. Viruses, worms and spyware can easily use these devices to enter your business. So, kindly use them carefully. You should use a firewall to protect computers that are connected to the outside world. Laptops and home workers will also need firewall protection.

Make regular backups of important work and data, and check that the backups were successful. You should also find a safe place to store you backups, perhaps even off-site in case of fire. If you are infected with a virus, you will be able to restore any lost programs and data.

The following ways can be used to protect:

1) Don't download executables and documents directly from the internet.
2) Don't open unsolicited programs, documents or spreadsheets.
3) Don't play computer games or use screensavers which did not come with the operating system.