During the dormant phase, **the virus has accessed its victim's computer or software**, but it does not do anything yet. The virus will wait until a "trigger" gives it the command to execute. This trigger could be anything from a predefined date to the user taking a specific action, like double-clicking an icon.

In the propagation phase, the virus is **fruitful and multiplies**. The virus will start to insert copies of itself into other programs or areas on the disk. These copies are often altered in some way to make detection more difficult.

The triggering phase is designated **when the virus changes from being dormant to being activated**. Finally, during the execution phase, the virus gets to work.

Execution phase. This is the actual work of the virus, where the **"payload" will be released**. It can be destructive such as deleting files on disk, crashing the system, or corrupting files or relatively harmless such as popping up humorous or political messages on screen.

A Parasitic Virus, also known as **a file virus**, is spread by attaching itself to executable programs. When a program infected with a parasitic virus is opened, the virus code runs. To hide, the virus passes control back to the original program.

A Memory-Resident Virus is **a virus that is located in the memory of a computer**, even after the 'host' application or program has stopped running (been terminated). Non-Memory-Resident Viruses are only activated once the application or program is started.

A boot sector virus is **a type of virus that infects the boot sector of floppy disks** or the Master Boot Record (MBR) of hard disks (some infect the boot sector of the hard disk instead of the MBR).

In computer security, a stealth virus is a **computer virus that uses various mechanisms to avoid detection by antivirus software**. Generally, stealth describes any approach to doing something while avoiding notice

Polymorphic viruses are **complex file infectors** that can create modified versions of itself to avoid detection yet retain the same basic routines after every infection. To vary their physical file makeup during each infection, polymorphic viruses encrypt their codes and use different encryption keys every time.

A metamorphic virus is one that can transform based on the ability to translate, edit and rewrite its own code. It is considered **the most infectious computer virus**, and it can do serious damage to a system if it isn't detected quickly.

A computer worm is **a type of malware that spreads copies of itself from computer to computer**. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage.

A Trojan horse is **a type of malware that downloads onto a computer disguised as a legitimate program**. A Trojan horse is so-called due to its delivery method, which typically sees an attacker use social engineering to hide malicious code within legitimate software.

Sniffing is the process in which all the data packets passing in the network are monitored. ... Sniffers can be hardware or software installed on the system. Spoofing is the process in which **an intruder introduces fake traffic** and pretends to be someone else (legal source or the legitimate entity).

Phishing is a **type of social engineering attack often used to steal user data**, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.























