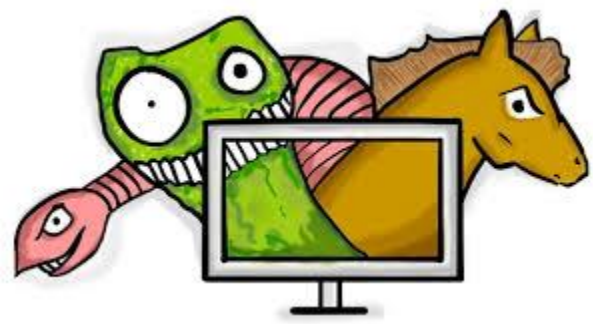
What is a computer virus?

A computer virus, much like a flu virus, is designed to spread from host to host and has the ability to replicate itself. Similarly, in the same way that flu viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document.

In more technical terms, a computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process, a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.



What are the different types of computer viruses?

1. Boot sector virus

This type of virus can take control when you start — or boot — your computer. One way it can spread is by plugging an infected USB drive into your computer.

2. Web scripting virus

This type of virus exploits the code of web browsers and web pages. If you access such a web page, the virus can infect your computer.

3. Browser hijacker

This type of virus “hijacks” certain web browser functions, and you may be automatically directed to an unintended website.

4. Resident virus

This is a general term for any virus that inserts itself in a computer system’s memory. A resident virus can execute anytime when an operating system loads.

5. Direct action virus

This type of virus comes into action when you execute a file containing a virus. Otherwise, it remains dormant.

6. Polymorphic virus

A polymorphic virus changes its code each time an infected file is executed. It does this to evade antivirus programs.

7. File infector virus

This common virus inserts malicious code into executable files — files used to perform certain functions or operations on a system.

8. Multipartite virus

This kind of virus infects and spreads in multiple ways. It can infect both program files and system sectors.

9. Macro virus

Macro viruses are written in the same macro language used for software applications. Such viruses spread when you open an infected document, often through email attachments.

How does a computer virus attack?

Once a virus has successfully attached to a program, file, or document, the virus will lie dormant until circumstances cause the computer or device to execute its code. In order for a virus to infect your computer, you have to run the infected program, which in turn causes the virus code to be executed.

This means that a virus can remain dormant on your computer, without showing major signs or symptoms. However, once the virus infects your computer, the virus can infect other computers on the same network. Stealing passwords or data, logging keystrokes, corrupting files, spamming your email contacts, and even taking over your machine are just some of the devastating and irritating things a virus can do.

While some viruses can be playful in intent and effect, others can have profound and damaging effects. This includes erasing data or causing permanent damage to your hard disk. Worse https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html e yet, some viruses are designed with financial gains in mind.

Data from: https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html

To know about Computer Virus more: A Brief History of Computer Viruses