**What is computer virus?**

The word virus comes from Latin and means “poison” or “slime.” Unpleasant as these terms are, they well describe the consequences when a computer virus infects your PC.

A computer virus is a malicious software program loaded onto a user’s computer without the user’s knowledge and performs malicious actions. In the worst case, a virus can cause a complete system failure.

Computer viruses can easily spread through the Internet and email, causing potential harm to a computer’s data, files and hard drive. Viruses are commonly disguised as hyperlinks, pop-ups or email attachments of images, greeting cards or audio or video files.

**How can you prevent a computer virus?**

one thing is certain: complete protection against computer viruses would only theoretically be possible if the PC were completely isolated from outside data. But that would mean avoiding the exchange of files via USB stick, CD or Internet. Therefore, this approach is not very practical.

One effective method in the fight against PC viruses is prevention, which requires caution when dealing with Internet sources. This means, for example, that email attachments or files from unknown sources should not be opened. In addition, you should use a spam and malware filter for your mailboxes.

If computer viruses reach your PC, an antivirus program can detect, block and combat the malware. The antivirus tools available on the market can be divided into three types: Real-time, manual and online scanners.

Since new forms of computer viruses with new virus signatures are constantly being created, anti-virus tools must always be kept up to date. It also makes sense to continuously update the operating system installed on your PC because there are often security holes in outdated operating systems that are a target for computer viruses. These security holes are often corrected in patches, which is why regular updates are so important.

Another form of virus detection is vaccination, where data is recorded in certain sections and stored in a special file. During subsequent checks, the last saved file is compared with the current status. If a discrepancy is found between the two files, the program alerts users to a possible computer virus infection.

In principle, it is advisable to make backup copies of all files so as not to lose data irretrievably in the event of a computer virus.

**Types of virus**

### 1. File-infecting Virus

A virus that attached itself to an executable program. It is also called a parasitic virus which typically infects files with .exe or .com extensions. Some file infectors can overwrite host files and others can damage your hard drive’s formatting.

### 2. Macro Virus

This type of virus is commonly found in programs such as Microsoft Word or Excel. These viruses are usually stored as part of a document and can spread when the files are transmitted to other computers, often through email attachments.

### 3. Browser Hijacker

This virus targets and alters your browser setting. It is often called a browser redirect virus because it redirects your browser to other malicious websites that you don’t have any intention of visiting. This virus can pose other threats such as changing the default home page of your browser.

### 4. Web Scripting Virus

A very sneaky virus that targets popular websites. What this virus does is overwrite code on a website and insert links that can install malicious software on your device. Web scripting viruses can steal your cookies and use the information to post on your behalf on the infected website.

### 5. Boot Sector Virus

These viruses are once common back when computers are booted from floppy disks. Today, these viruses are found distributed in forms of physical media such as external hard drives or USB. If the computer is infected with a boot sector virus, it automatically loads into the memory enabling control of your computer.

### 6. Polymorphic Virus

This virus has the capability to evade anti-virus programs since it can change codes every time an infected file is performed.

### 7. Resident Virus

A resident virus stores itself on your computer’s memory which allows it to infect files on your computer. This virus can interfere with your operating system leading to file and program corruption.

### 8. Multipartite Virus

A type of virus that is very infectious and can easily spread on your computer system. It can infect multiple parts of a system including memory, files, and boot sector which makes it difficult to contain.

**How do you know your computer is infected with a virus?**

When it comes to determining if your computer is infected, there are many things that you should look for. Here are some signs that your computer may have a virus.

### 1. Computer Running Slowly

One of the most common things that viruses do is make computers run slowly, especially when you open programs or files. This might cause your computer to freeze and not respond to anything you do. Viruses can consume a substantial amount of your system resources leading to high CPU usage. Sustained high CPU usage can make your CPU hotter than expected, leading to sluggish performance. You may also notice that your fan is running louder than normal. This is because the CPU is working harder to keep the system cool, thus using more power.

### 2. Strange Pop-Ups on Screen

If you see pop-ups you didn’t authorize, it’s probably because your computer has a virus. These pop-ups can be annoying messages that contain malware. The messages might say that your computer has been infected and that you need to call a certain phone number in order to fix the problem. Such messages might also contain a link that will take you to a website that will supposedly fix the virus.

### 3. Unwanted Programs or Toolbars

Viruses can try to install additional programs or toolbars without your consent to give criminals access to your system. If you notice that there are new programs on your computer have you don't remember installing, or your browser toolbar has changed, it could indicate a virus. Also, if you start seeing unfamiliar icons on your computer, that could be another sign of a virus. The icons might have a question mark on them, and they might look different from the standard icons on your computer.

### 4. Files Disappearing

If files are disappearing from your computer without your permission, there is likely a virus on your system. The virus may have deleted the files, or a hacker might've encrypted them and is holding them for ransom. Similarly, if you see messages that say that certain system files are corrupted, your computer may have a virus. This can cause the computer to crash or freeze. Sometimes it’s email messages that disappear. If you’re unable to find emails that you were expecting, then a virus might have deleted them from your inbox. This is especially true if you don’t remember deleting them yourself.

### 5. Antivirus Not Working

If the antivirus program that you have installed on your system isn’t working, it’s possible that a virus deleted or disabled it. Viruses can disable your antivirus program by disabling it from the system registries. Viruses can also access and modify your antivirus software’s configuration settings, thus altering the instructions from the registries. Once the malware disables the program, it will allow itself to run without the antivirus scanning it. This leaves your computer susceptible to further attacks.

### 6. Spam Coming In From Unknown Sources

Are you receiving spam emails from addresses that you don’t recognize? Your computer may have a virus. This is because viruses can send out emails from your address without your consent. One of the main ways computers become infected by a virus is through spam email. These emails often contain a link to a fake website, and if you click on them, an executable file will download onto your computer. This executable file is the virus itself, and it’s what installs the infection onto your system.

If you see any of the above signs, it’s important to take steps to scan for viruses and remove them from your computer as soon as possible.

**What is an antivirus?**

Antivirus is a kind of software used to prevent, scan, detect and delete viruses from a computer. Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks.

**What is malware?**

Malware, short for “malicious software,” refers to any intrusive software developed by cybercriminals (often called “hackers”) to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware. Recent malware attacks have exfiltrated data in mass amounts.

**what are the types of antivirus?**

All antivirus programs can be organized into the following three categories:

1. Standalone Antivirus Software

Standalone antivirus software is a specialized tool designed to detect and remove certain viruses. It is commonly referred to as portable antivirus software because it can also be installed on a USB drive and used by administrators to run an emergency scan of an infected system. However, most portable programs aren’t designed to provide real-time protection and download new virus definitions daily, which is why they cannot substitute internet security suites that include a variety of additional features.

1. Security Software Suites

As mentioned above, security software suites are more than just antivirus programs. In addition to being able to detect and remove viruses, they are also equipped to fight all other types of malicious software and provide round-the-clock protection for your computer and files. Most of these program packages include anti-spyware, firewall, and parental controls features. Some also include additional functionality like password managers, a VPN, and even a standalone antivirus program bundled with the suite.

1. Cloud-Based Antivirus Software

Cloud-based antivirus software is a fairly new type of antivirus technology that analyzes your files in the cloud rather than your computer in order to free up your computational resources and allow for a faster response. These programs typically consist of two parts – the client that is installed on your computer and runs periodic virus and malware scans without taking up too much memory and the web service that processes the data gathered by the client and inspects it for matches in its virus and malware database.

**How to choose computer antivirus?**

The market is flooded with antivirus programs that claim to provide optimal protection for your computer, your files, and your personal data. With such strong competition, finding the best antivirus software may prove difficult.

You pay more attention to their features, including the number of devices they can protect, the operating systems they support, the speed, and so on, all of which can affect the security of your system.

Another point that should be taken into consideration is that you should consider your budget while choosing an antivirus. You can use the paid types if you have enough budget to get an antivirus because they certainly have more features than free ones. Still, if you have a limited budget, you can look for the best type of free antivirus programs that has features which are somehow same as the paid ones.

When it comes to choosing the best antivirus for your system, you need to pay attention to the amount of time that these programs take to scan, detect and eliminate existing viruses and malware in your system if they can control your system only for a few hours, it is better not to select them and choose the ones that can monitor and control your system for many hours throughout the day.

**How antivirus work on your computer?**

When a [computer virus](https://www.computerhope.com/jargon/v/virus.htm) infects a computer, it must make changes to [files](https://www.computerhope.com/jargon/f/file.htm), critical areas like the [registry](https://www.computerhope.com/jargon/r/registry.htm), or sections of [memory](https://www.computerhope.com/jargon/m/memory.htm) to spread or damage the computer. An antivirus program protects a computer by monitoring all file changes and the memory for specific virus activity patterns. When these known or suspicious patterns are detected, the antivirus warns the user about the action before they're performed. Below is a list of the different forms of virus detection an antivirus can use to protect your computer.

## Heuristic-based detection

The most common form of detection is a [heuristic-based detection](https://www.computerhope.com/jargon/h/heuristi.htm) that uses an [algorithm](https://www.computerhope.com/jargon/a/algorith.htm) to compare the signature of known viruses against a potential threat. Heuristic-based detection can detect viruses that have not yet been discovered. It may also detect known viruses that were modified or disguised, and released into the wild again. Heuristic-based scanning is the best-known method for detecting new viruses. However, it can also generate false positive matches, which means an antivirus scanner may report a file as being [infected](https://www.computerhope.com/jargon/i/infect.htm) that is not infected. These "false positives" are minimal, but not uncommon.

## Signature-based or virus dictionary detection

Every antivirus scanner has a virus [definition file](https://www.computerhope.com/jargon/d/definiti.htm), database, or dictionary containing thousands of known virus signatures. These signatures allow an antivirus program to identify past viruses that were analyzed by security professionals. Today, there are well over 100,000 different known virus signatures that can be used for comparison. Signature-based detection is an excellent way to prevent past known viruses and is the best method of detection without creating a false warning. However, signature-based detection cannot detect new viruses until the definition file is updated with new virus information.

## Behavior-based detection

If a virus has made it past the above detections, the antivirus analyzes the behavior of programs running on the computer. If a program begins to perform strange actions, the antivirus may trigger a warning. Below are examples of the types of actions and behaviors that may trigger a warning.

* Changing settings of other programs.
* Modifying or deleting multiple files.
* Monitoring keystrokes.
* Remotely connecting to computers.

Behavior-based detection is a useful method of finding viruses or other malware that attempt to steal or log information. However, many programs today need to report to an online server or log keystrokes to prevent online cheating, sometimes causing this type of detection to create false warnings.

## Sandbox detection

If a program is suspicious, some antivirus programs can also use [sandbox](https://www.computerhope.com/jargon/s/sandbox.htm) detection, which creates an emulated environment for the program to run and analyze its behavior. When executed in the emulated environment, if the program appears to perform destructive or abnormal behavior, the antivirus alerts the user before running it.

## Cloud antivirus detection

Cloud antivirus detection uses a computer program that collects information, which is then uploaded and processed by a server in the [cloud](https://www.computerhope.com/jargon/c/cloudcom.htm). By running all detection on the server, your computer is spared additional processing. Cloud antivirus requires an Internet connection.