User's guide to avoiding virus infections
Keeping an eye out for viruses

---
---

---
---

Computer viruses are everywhere! This guide will show you how to stay alert and how to avoid getting infections on your computer. Having an updated virus scanner is only a small part of this, there are many ways that you can prevent having viruses other than a virus scanner, as it will not always save you.

Types of viruses
There are many type of viruses. Typical viruses are simply programs or scripts that will do various damage to your computer, such as corrupting files, copying itself into files, slowly deleting all your hard drive etc. This depends on the virus. Most viruses also mail themselves to other people in the address book. This way they spread really fast and appear at others' inboxes as too many people still fall for these. Most viruses will try to convince you to open the attachment, but I have never got one that tricked me. In fact, I found myself emailing people just to make sure they really did send me something. It does not hurt to be safe.

Worms
Worms are different type of viruses, but the same idea, but they are usually designed to copy themselves a lot over a network and usually try to eat up as much bandwidth as possible by sending commands to servers to try to get in. The code red worm is a good example of this. This worm breaks in a security hole in Microsoft IIS (Internet Information Server) in which is a badly coded http server that, despite the security risks, a lot of people use it. When the worm successfully gets in, it will try to go into other servers from there. When IceTeks was run on a dedicated server at my house, there was about 10 or so attempts per day, but because we ran Apache, the attempts did not do anything but waste bandwidth and not much as I had it fixed a special way. Some worms such as the SQL slammer will simply send themselves over and over so many times that they will clog up networks, and sometimes all of the internet. Worms usually affect servers more than home users, but again, this depends on what worm it is. It is suspected that most worms are efforts from the RIAA to try to stop piracy, so they try to clog up networks that could contain files. Unfortunately, the RIAA have the authority to do these damages and even if caught, nothing can be done.

Trojans
Trojans are another type of virus. They are simply like a server in which enables hackers to get into and control the computer. A trojan such as Subseven can enable a hacker to do various things such as control the mouse, eject the cd-rom drive, delete/download/upload files and much more.

MBR virues
Boot sector viruses are another type, they are similar to file viruses, but instead they go in the boot sector and can cause serious damage when the computer is booted, some can easily format your drive simply by booting your computer. These are hard to remove.

Most viruses have various characteristics. For example, a worm can also be a trojan and also infect the boot sector. It all depends on how the virus is written and what it is designed to do. That's why there are not really strong structured categories, as they can easily mix one in the other.

Know the potentially dangerous files

Like any other files, viruses must be opened in order to do something. Most viruses come through e-mail as an attachment. Some will make it look like it's someone you know, and it will try to convince you to open an attachment. Never open attachments at any cost! Some viruses will infect files in programs, so opening a program will actually open the virus, maybe the same one, or another part of it.

All files have what is called an extension; This is the 3 last letters after the last period. For example, setup.exe has a file extension of .exe.

Extensions to watch out for are .exe .com .bat .scr .pif .vbs and others, but these are the most seen. .exe .com .bat .pif and .scr are valid extensions for executables. A virus writer will simply rename it to one of these and it will work the same way. .pif is a shortcut to an ms-dos program and will have the ms dos icon, but will still execute whatever code is in it, so an .exe can be renamed to .pif and be run the same way. .bat is a batch file, which can contain instructions to do various file activities, but again, a .exe can be renamed to .bat and it will execute it! .vbs is a visual basic script. For some reason, Microsoft provides this scripting language along with the scripting host to make it more convenient to design and write viruses quickly and easily, I've never seen another use for this scripting language other than for writing viruses. There are programs that are written with that language, but it is compiled into an exe. Exe is the usual extension for programs, you would not have a software CD install a bunch of vbs files all over!

Bottom line is, if you don't know what a file is just don't open it. Some viruses will sometimes be named a way as to mask the real file extension to make it look like a harmless file such as a image file. This is easily noticed, but can still be missed. Simply don't open unexpected files.

If you get something that appears like something legit, just ask the person it came from if they sent it. Most viruses use a friend's address to make it look like it comes from them. The virus does this by using the person's address when sending itself to the address book contacts.

Downloads

Email is not the only way to get viruses; P2P (file sharing programs such as kazaa, winmx, direct connect etc) is also another way to get viruses.

When downloading programs, the main thing to watch out for is the file size. If you are downloading a program that you expect to be rather large such as a game, don't grab a file that is 10KB, since it's most likely a virus. However, I've been caught with a virus even with large files, so file size is not the only thing to watch, as an exe is still valid even if junk is added at the end, so a 64KB virus will still function even if it is turned into 650MB.

Icons are something to look for too, fortunately, virus writers don't take time to put icons. If your download should be a setup file, you should see the icon of a setup file. If it's just the blank icon that typical plain or corrupted exes have, don't open it.

Another thing to do, which should be obvious, is to scan the file for viruses using updated virus definitions. But don't rely on only your virus scanner, as they are not perfect, and if the virus has not been reported to them yet, they won't know to create a definition for it!

## Changing settings to stay safe

If you do open a virus, you want to avoid it going to all your friends. The simplest thing to do is to NOT use the windows address book. It is easy for viruses to get through and Microsoft is not doing anything about it. Just don't use it. Put them in spreadsheet or even better write them down somewhere. Don't use the address book.

Another "feature" to avoid is the auto preview. Some viruses can attempt to open themselves just by opening the email. There are security holes in Microsoft mail programs that allow this. In Microsoft Outlook, click on the view menu and remove auto preview. You need to do this for every folder, but the inbox is most important. In Outlook Express, click on the view menu and go to layout. In the dialog box, you will see a check box for show preview pane. Uncheck it and click ok.

Another thing you should change, especially if you download a lot, is the option that allows you to view the file extension. In Win98, go in any folder, click on view then folder options and choose the view tab and where it says hide file extension for known types, uncheck it. In win2k, it is the same process, but instead, go in the control panel and open the folder options icon.

## Avoiding server worms

Some viruses, mostly worms, can exploit through servers and affect other servers from servers that have been infected. A good example is the SQL slammer. This was a worm that affected SQL servers run by Microsoft IIS and Microsoft SQL Server. Once the worm gets in, that particular server starts trying to find more exploitable driving internet connections to a halt in the process. Servers running Apache were unaffected by that, except for the many hits to try to get in. IceTeks received about 100 hits per day when it was run on a dedicated home server. Most hits came from major ISPs and other big websites that had no clue they were still affected.

The simple solution to avoid these types of viruses is to NOT use Microsoft based server software for your server, especially if it is a public server. The operating system is also crucial, but the actual server software is much more. Apache, which is free, is much more secure than Microsoft based server programs such as IIS. IIS may be easier to understand and administer, but it saves a lot of hassle to learn how to use Apache. IIS has a large number of vulnerabilities, such as the ability to gain access to cmd.exe and basically delete the whole drive by doing a ../ request in the address bar. These don't require viruses, but simply commands, but there are worms written to automatically make these commands. The code red does this.

## Removing a virus

The best way to do this is to do a clean install. However, depending on how bad the virus is, a simple clean install won't remove it. So to be extra sure, you'll want to do a low level format. This is especially true of you got a boot sector virus, as even repartitioning and formatting won't quite remove it, but sometimes you can get away with an fdisk /mbr, but not all the time. here are various removal tools for viruses, it is good to use them and see if they work, but proceeding with the clean install is recommended. You never know if the virus is completely removed by deleting files you suspect are infected. Some viruses such as the Bugbear will close anti virus programs and other programs to make it hard and annoying to figure out what to do. A clean install is the best way to ensure that it's gone for good.

Viruses are out there, don't be one of the many infected ones! Stay alert and stay safe! Don't open unexpected files, regularly update your virus definitions and scan downloaded files!

I hope this article was useful for you!