

# Virus Presentation

What is a Virus?

A virus is like any other computer program you are currently using &hellip;&hellip;with one major difference&hellip;&hellip;It has the unique ability to replicate. Viruses can attach themselves to just about any type of file and are spread when these files are copied and sent from individual to individual. Viruses won&rsquo;t go away any time soon. The most recent information has indicated that there is a new virus created every four minutes. With numbers like these, it&rsquo;s safe to say that most organizations will deal regularly with methods to reduce the risk of viral infections. No one who uses computers is immune from viruses.

The SIX STEPS in the lifecycle of a virus.

1. Creation&hellip;It used to be that you had to be a fairly sophisticated programmer to create a virus, now just about anyone with a little programming knowledge and a warped personality can create a virus.
2. Replication&hellip;&hellip;.A truly mean virus will be programmed to replicate quietly for a long period of time before it activates. This gives it a chance to attach itself to a large number of files.
3. Activation&hellip;&hellip;.Viruses that contain damage routines will activate when certain conditions are met, for example, on a certain date or when a particular action is taken by a user. Viruses without damage routines create problems by stealing storage space and memory, resulting in the downgrading of the overall performance of your computer.
4. Discovery&hellip;&hellip;.This phase doesn&rsquo;t always come after activation, but it usually does. When a virus is detected, it is isolated and sent to the Int&rsquo;l Computer Security Assoc. in Washington DC to be documented and distributed to antivirus developers. What astounded me was that this discovery usually takes place at least A YEAR before the virus might have become a threat to the computing community.

This means that if you are getting viruses, the true culprit may have more to do with your current virus prevention process than the actual risk level of infection. With a small attention to regular maintenance procedures, you should be able to protect yourself at work and at home with very little effort.

5. Assimilation&hellip;&hellip;.At this point, antivirus developers modify software so that it can detect a virus. This does NOT only occur with antivirus specific software. All updated versions of Microsoft operating systems will contain patches that also help to reduce your computer&rsquo;s vulnerability to viruses.

6. Eradication&hellip;.If enough users install up-to-date virus protection software, any virus can be wiped out. So far no viruses have disappeared completely, but some have ceased to be a major threat.

So what happens when you get a virus?

The best scenario is that your anti-virus software finds and eliminates it. An example of this would be that a virus came attached to an email. When the email is being received, the virus scanner detects the virus and cleans it (removes the virus parts and leaves the information). If it can&rsquo;t clean it, the attachment portion of the email is deleted. The antivirus software can do this because it is programmed to look for &ldquo;Virus Definitions&rdquo;. These are virus signatures that have been identified and the software is designed to delete any code that matches these definitions.

Why does your antivirus software seem to catch some viruses and miss others? What do you do now?

As mentioned before, your antivirus software is made up of programs that are designed to check incoming code against known virus definitions. When it finds a match, the software goes to work cleaning or deleting the file. With a virus being created every 4 minutes, there is a chance that you will receive one of these new viruses BEFORE you receive the software upgrade that adds this particular set of definitions to your antivirus check list.

Here&rsquo;s the kicker. Because you have already been infected by this new virus, even when you receive the online update to your software, you load them, and the software is set to check all incoming email, this virus will continue to contaminate your system. Why? Because it was already in your system by the time your software was given the virus definitions! The software is set to check NEW email from the time it is loaded and forward into the future. It is not checking all your current files.

To minimize the damage done by new viruses that sneak in ahead of the antivirus updates, you must have a regularly scheduled scan of the vulnerable areas of your system. This will catch and delete those viruses that get by you. It is more than possible that you will have a virus in your system and be totally unaware that it is damaging your data until it activates. Viruses today are programmed to send pre-scripted email messages to every file in your address book. They are also programmed to then bypass the SENT ITEMS log, leaving no trace of their existence. Unless you actually see the nanosecond flicker when it sends, you may have no idea that your system is infected people. Regular running of your antivirus software AS WELL AS real time email checks will limit your risk of infection. How often you run a check and on what files depends on the size of your business and the amount of outside communication that occurs.

What do you do if you get a virus and you do not have antivirus software?

Believe it or not, the WORST thing you can do at this point is install antivirus software and expect it to eliminate the virus. When you do this, the virus will attach itself to (infect) the antivirus software before it can run and may cause damage to the antivirus program. So even though you have installed antivirus software, it is no longer able to operate properly and needs to be completely removed and reinstalled. The trick is that the antivirus software may be difficult to uninstall completely due to the damage caused by the virus and your system is left vulnerable to infection.

The best thing to do is an online antivirus scan. This offers you the most up to date antivirus software, and if it detects something it will clean it immediately. THEN RUN (or click) and buy antivirus software before any other viruses get an opportunity to infect your system.

How can you protect yourself?

One of the most critical things you can do is to keep your operating system software at the most current update available from the manufacturer. For as long as the manufacturer supports your version (e.g.: Windows 98) your operating system software will generally come with free on-line updates that include new code that may help block virus entry. You should be checking for updates as part of your regular maintenance routine. This will not only help to protect you from viruses, but it will also ensure you are getting the most from your software investment as the updates may include patches that make an awkward function more user friendly. Be aware that even though these updates are available for everyone, if you are not running licensed software, downloading one of these updates may end up disabling the software you are using.

It is also important to install licensed anti-virus software and set it to run automatically during the evening or early in the morning on a regular basis. We run ours once a week. Installing anti-virus software can only protect you

-

if it's SET to check every communication that comes into your system in real time

-

if it is SET to check ALL your vulnerable files on a regular basis.

-

if it's CURRENT

(we receive updates on PC-cillin at least 4 times a week always say YES you want to update immediately, it won't interfere with the work that is up on your screen, and it doesn't take long)

All three steps are critical in getting the most from your antivirus software.

Lastly, be aware of the emails you are receiving before you open them and train everyone who comes near any computer workstations on what to do if they see a suspicious email. Today's viruses can be activated just by clicking on the new email and previewing its contents. If you have Outlook Express it does not allow you to turn off the preview window so you need to RIGHT click on the suspicious email and hit the DELETE option.

One other area in which your computer system is vulnerable relates to the existence of spy-ware programs.

These lovely pieces of software have various forms of entry. They can come into your system attached to emails, from web-browsers like internet explorer or Netscape, or from file sharing programs like Kazaa. Once imbedded inside your computer they will collect data regarding your web browser patterns, where you go, what you look at, what you buy, and anything else their creator deems important. This information is then made available at a price to marketing firms and any other interested parties. Although this is valuable information at one level it is certainly offensive at another, and it does not end there. Spy-ware programs open a portal into your computer system and provide a gateway for hackers to enter your business and have access to all your data... financial, proprietary, and communications at all levels of your organization. There is a free software package that can be downloaded and installed that will search your computer for these files and eliminate them.

Virus protection is a critical component of your computer system maintenance.

Due to the high risk of infection, you would not be allowed to travel to Africa unless you were properly vaccinated. Think of your computer as a vehicle for traveling data. Without virus protection and a regular maintenance schedule, the risk of viral infection increases exponentially and you may be jeopardizing one of your company's second most important asset - its data.

At GCS Systems, we encourage you to talk to us or to your current tech support company about regular maintenance.

In a number of cases, a good tech company can analyze your system and design a step by step procedure that your own staff can follow as part of their responsibilities. This not only offers you all the benefits of a well maintained computer system, but also gives your tech support company a point person who is familiar with your system and who can help minimize any troubleshooting time when your system is down. This of course will save you money.