

---

## Keep Backup Copies

Computer viruses and equipment failures can result in unusable files. If a hard disk or removable media disk is unusable, there may be no way of restoring the file to a usable state, except through a backup copy. However, a backup may be of little or no value if it is also damaged or infected with a virus. ITS recommends the methods described below for backing up disks and/or files.

Use a virus detection program to search for any known viruses that might be on the hard disk or the removable media disk containing the files to be backed up. If a virus is found, remove the virus before backing up the files. This precautionary measure reduces the possibility of performing an infected backup.

Another method is the staggered backup strategy -- a routine of backing up data and document files on an incremental basis to increase the possibility of having a good set of backup disks. For example, keep two sets of backup disks, set A and set B. The first time, backup data and document files to the set A disks. The next time, use the set B disks.

Additionally, backup the operating system each time a modification is made, application and program files each time default configurations are modified, and data and document files each time current versions are updated.

## Never Work From A Master Disk

Computer viruses are unable to infect files on write-protected or locked disks. A 3.5" floppy disk can be write-protected by snapping the lock tab. Zip disks can be write protected by using the Zip tools utilities included with zip drives (also available on the web).

### For Additional Information...

For information on obtaining free antiviral protection programs and definition files, see the Technology Self Help pages at:

<http://www.bgsu.edu/its/tsc/self-help/>

and select the topic 'Virus Protection'.



For comprehensive information on computer viruses and suggestions for keeping your personal computer secure see:

<http://www.bgsu.edu/its/security/advice/page11132.html>

Check the link "ITS Security Alerts" for recent virus advisory warnings for the campus community.

# Computer Viruses



*Bowling Green  
State University*

Information Technology Services  
209 Hayes Hall - BGSU  
419-372- 2911  
<http://www.bgsu.edu/its/>

## What Are Computer Viruses?

Any program that has the ability to reproduce and attach itself to other programs is referred to as a computer virus. Computer viruses can spread to a hard disk or removable disk whenever an infected computer program or system is used and the uninfected disk is accessed. Listing directories, executing programs, printing files, and starting computers are examples of accessing a disk.

In addition to being able to reproduce, viruses may be designed to perform different destructive functions. For example, computer viruses may:

- Display unexplained messages
- Delete specific files
- Erase all of the files that are stored on a hard disk or a floppy disk
- Make entering from the keyboard difficult or impossible
- Modify data and document files
- Modify the File Allocation Table
- Modify the Boot Sector
- Add extra files to a disk
- Cause problems printing
- Cause frequent system failures
- Cause problems displaying fonts

After viruses infect files, they may wait for a signal before performing their destructive tasks. There are two types of signals that may invoke viruses to perform destructive tasks; *time bombs* and *logic bombs*. *Time bombs* are signals activated by a specific time of day, date, or hour. *Logic bombs* are activated when specific functions are performed.

## Types of Computer Viruses

Viruses may be on systems for weeks or even months before symptoms appear. However, the sooner viruses are detected, the fewer applications, and systems will be affected.

If your computer experiences frequent system failures, unexplained difficulties in printing, slower operation, and/or the inability to run certain or all applications, a computer virus may be the cause. This does not mean that viruses are definitely the cause of problems, but they should be checked immediately.

Some of the most common types of viruses include: worms, boot viruses, macro viruses, and virus hoaxes.

- |                    |   |
|--------------------|---|
| <b>Worm</b>        | Destructive programs that replicate throughout disks and memory, using up computer resources and eventually bringing the system down.                   |
| <b>Boot Virus</b>  | Viruses written into the boot sectors of disk. If the disks are booted, they infect the system.   |
| <b>Macro Virus</b> | Viruses written in a macro language and placed within a document. When the document is opened the macro language executes the destruction or the prank. |
| <b>Virus Hoax</b>  | Phony warnings sent out by pranksters to upset as many people as possible.  |

## Staying Virus Free

There are several precautionary measures used to safeguard against possible infections. Following these methods will not prevent a virus from infecting a hard disk or removable media, but it will reduce the chances.

### Run Virus Checks Frequently

Viruses should be detected as quickly as possible so they do not spread to other systems.

ITS offers free virus protection software to the BGSU community, for both Macs and PCs. After downloading and installing these programs, ITS recommends running frequent virus scans on hard disks and removable disks.



### Update Virus Definition Files

Antiviral programs are useful only against known viruses. As new viruses are discovered, companies that make antiviral programs release new virus definition files, sometimes referred to as “DAT” files, to detect, remove, and protect against these new viruses. *You must use the most current virus definition files to guard against newly discovered viruses.* As new virus definition files are released, ITS makes them available to download from the ITS Virus Information page. Additionally, some antiviral programs are able to discern when their definition file becomes outdated, and will prompt you to update it.