

# Protecting your Computer from VIRUSES and Other Threats

By Michelle Lattke for New Tampa Technology  
11/6/05

*A VIRUS is a program that when run on your computer deletes files, changes settings, etc. in a negative fashion and often time spreads itself to others connected to you via a network. Different viruses have different effects on your computer; some are more serious than others. Many current viruses are written to affect PCs running the Windows platform and email users using Microsoft Outlook.*

## HOW DO YOU PROTECT YOUR COMPUTER???

1. Buy a virus protection software and keep it up-to-date! [Norton Anti-Virus](#) is a good product, as is [McAfee](#). Both run between \$40-\$50 each year. You can buy most virus software at office supply chains, electronics stores, or your favorite computer software dealer (e.g. Staples, Wal-Mart, Best Buy). Keeping the virus definitions up-to-date is as important as buying and installing the software. If you don't, you will be unprotected from new viruses. Most virus software can be set to automatically update it's virus definitions from the Internet, but in order for this method to be effective, you must not cancel the updates when they are in progress, because you find them annoying or time consuming.

For home use, you can also download a free virus protection software (remember you often get what you pay for) called AVG from <http://free.grisoft.com> or Anti-Vir from <http://www.free-av.com/>. These versions can help you with home use, but are not licensed for commercial or business use. The only free anti-virus software that is free for commercial use is [ClamAV](#) which is an open source virus protection tool which can be downloaded from <http://sourceforge.net/projects/clamav/>.

The bottom line with viruses is that an ounce of prevention is worth more than a pound of cure. If you rely on information or files on your computer, you must invest in virus protection.

2. Avoid unwanted and/or harmful downloads while surfing the Web. Don't download files or programs from companies or websites you don't recognize. AND if you ever decide download something from a website that you trust, don't do it from an email link; type the link into a web browser yourself, so that you are sure you are going where you intend to go.

When you go to a website, and a window pops up with some message about how you need something to view the page properly, READ THE MESSAGE. Do not automatically assume that it is okay to download. Unless it is something like Flash Player or Acrobat Reader, you probably don't NEED it, and it will probably only serve to bog down you computer.

It has also become commonplace these days for spammers to send you messages that look like they are from real companies (like PayPal or your credit card company or Microsoft), but they are really copycat fakes whose links take you to erroneous places where they will install spyware or try to get you to give out personal information. The best bet if you get such an email is to close the email and to open a web browser, type in the website of the company in question and contact them through their company email or phone number. Never under any

circumstances should you give out username, password, or credit card information to someone over email.

Avoid pop-up ads by using a simple pop-up blocker. Many browsers have built in pop-up blockers that you just have to turn on (e.g. [FireFox](#), Safari). Other companies offer browser plug-ins that block pop-ups; for example, Google offers a pop-up blocker in their useful [Google Toolbar](#).

If you do find yourself plagued by pop-up ads and spyware from previous indiscretions, consider downloading a program like [AdAware](#), which will identify and eliminate adware, spyware, and harmful cookies from your computer. It is free, and if you make the effort to run it regularly, you will go a long way to protecting your computer from damage.

3. Don't open email attachments from people you don't know or unexpected attachments from people you do know. You can't get a virus from reading the TEXT of an email. You can get a virus from opening an attachment from an email.

Although many people these days know to avoid attachments from people they don't know, they aren't as cautious about attachments from people they do know. Many viruses that are passed through email attachments can place any email address that they've gotten from victims address books in the "From:" line. So just because it says it's from your grandma or your friend Susie, doesn't mean that it is. To be safe, you shouldn't open an attachment unless that you know that it is coming and you know what it is or unless you have checked with the person who sent it, so you know that they meant to send it to you.

4. Don't put a floppy disk or CD in your computer if you don't know where it's been. No one would chew a piece of gum found on the ground; we all know that is totally gross. So think of that when you get a disk from someone. Do they have virus protection on their computer? Will any of their computer infections spread to your computer through this disk?
5. Check out virus alerts you get via email before passing them on...MANY are hoaxes. At Symantec's Security Response website, <http://securityresponse.symantec.com/>, you can type the subject of the email or the supposed name of the virus into the search box, and their experts will tell you all that you need to know about the threat. Ensure that the time you spend worrying about viruses is on actual threats as opposed to someone's idea of a joke.
6. Keep your Operating System up to date. Many viruses and worms prey on security holes in your computer's operating system. On a PC, regularly run [Windows Update](#) to take advantage of any security fixes for your operating system that might be open doorways to a virus or worm. On a Mac, run Software Update under the Apple Menu to check for updates.
7. Backup, backup, and backup again! Backup is just techie speak for make a copy of the file somewhere else. The reason you get virus protection is to protect both your computer and the precious files that are on it. An important additional protection is to backup your critical files to an external source, such as a CD, DVD, or external hard drive/thumb drive. It takes only a few minutes to do this on a regular basis and will save you many tears should your computer crash or become irreparably infected by a computer virus.

8. If you do have a virus or think you have a virus, and you don't have protection or your protection won't fix the problem, try looking for a patch or cleaner tool. Often times, virus software companies or other computer-related companies will offer a free patch or virus cleaner tool which will fix one specific virus for you (e.g. Symantec, Microsoft, McAfee). Be cautious where you get the fixer tool from, however. Sadly, some people distribute tools that just cause more damage; be sure to get such a tool from a trusted source.

Keep in mind that this is an emergency backup option, because although such specific tools may eradicate the virus, you may lose some important files along the way. Virus prevention and detection software combined with pop-up and spyware removal and regular backup is the best way to go.