



Protecting your computer from VIRUSES

This sheet with in depth instructions can be found at:

www.ActionOneComputers.com

- **No anti-virus protection software can keep you 100% covered from viruses.** Viruses are put out faster than the anti-virus protection programs can keep up with them.
- **You should have VIRUS AND SPYWARE protection.** Spyware enters your computer and then shows the viruses how to enter.
- **Make sure your anti-virus software is configured to run a complete scan of your system at least once a month.** Yes this takes hours but it is worth it! Note with laptops since it prolongs the life of the computer to turn it off when not in use, you will most likely have to do a manual start of your virus scan once a month. Use an anti-virus package that supports regular, automated updates to include known viruses. (Avg does these up dates...that is why your computer may run slower when you turn it on for the first few minutes. You will still have to start a scan manually once a month.)
- **Slow down and read** the pop up before you just click to get rid of it.
- **Virus warnings are many times nothing but hoaxes—and viruses in and of themselves. Do not click on any portion of this pop up!** (See next note on how to close these.) If you believe you may have a virus close the notice in the manner below and open, up date and run your antivirus program. This way you are sure it is your antivirus running and you are not downloading damaging materials.
- **Close ALL pop ups properly. While you are on line if something pops up on your screen you did not ask for: DO NOT TOUCH THE BOX THAT POPPED UP!** Close this box by pressing these two keys at the same time (Alt +F4). This closes the last thing that was opened. Viruses are being downloaded by users unknowingly by clicking the X to close and by clicking on other buttons on the pop up, such as when you see options like “help, decline, no thanks, accept, close, yes or no”. If the pop up did not go away and you are leery of it you are better off to turn your computer off by pressing the off button until your computer shuts down. You can then restart the computer.
- **Be careful while doing internet searches.** Be especially careful when searching for things that may have "seedy" connotations, such as sex, drugs, etc. There is a practice whereby a hacker attracts a click by using somewhat benign keywords, then links the search result to a malicious website. These are hacker's favorite places to place viruses. They are most often related to non-business-related websites, however (entertainment, sex, drugs, etc.). Pay special attention to the wording returned by the search engine, and to the web address destination in the status bar (the gray bar just above the tray). Viruses have now become so prevalent that, given a choice, I will visit the website with the more well-known name (such as the National Institute of Health, rather than some no-name health website). If your computer has AVG for anti virus protection use GOOGLE as your search engine. It will prescreen the web pages for you. You will notice a green star with a white check on them after the site name if the page is virus free.

- **Any web site that allows you to download free music, etc., can pose a great threat. DO NOT USE THEM!!**
- **Facebook has viruses being attached to the links posted.** For example, if someone sends you a message “Look at this crazy cat video” and all you have to do is click on the blue type to see the video. When you hit the link viruses are attaching to them. A safe way to see the video is to highlight the address and paste into your address bar and go to it from there.
- **Do not go on line looking for free anti virus and spyware protection!** Some of these are viruses. For antivirus protection we suggest AVG 2012 and for spyware we suggest Malwarebytes. Both of these are free: Avg is found at <http://free.AVG.com> and Malwarebytes at www.malwarebytes.org (Make sure you are downloading the free version and only Malwarebytes or Avg. There are ads on the download pages that can be confusing and are NOT the product you want.) **Malwarebytes will need to be run manually once a month.** See the Malwarebytes manual at www.ActionOneComputers.com under resources.
- **Don't disable your anti-virus software** unless it's necessary for installation or removal of a program (some installation programs can look like a virus). If you do disable virus protection, re-enable it before connecting to the Internet, or reading a floppy diskette or a CD.
- **Don't open email attachments from people you don't know** and be wary of unexpected or unusual emails from known parties.
- **Don't open emails that have been forwarded unless necessary.** Those jokes and political emails are fun to read but the more they are forwarded the higher the chances they have viruses attached.
- **Another email precaution: You should never click on and run—or execute—any attachment file ending in .exe, .com or .bat without first checking with the sender.** See if it was his or her intention to send the file and, if so, whether the program has been checked and verified to be safe. This is especially important when you don't know the sender.
- **Email Virus Alerts—Can Be Viruses Themselves!**

The messages often go something like this:

VIRUS ALERT!!!

If you receive an e-mail with the title "Good Times", do not open it! It contains a virus which will wipe out your whole hard drive. This virus warning was issued by IBM and Microsoft. Send this warning to everyone you know!!

These virus warnings are many times nothing but hoaxes—and viruses in and of themselves. Although they do not execute malicious code to wipe out hard drives, they often get people to send massive quantities of e-mail to everyone in their address book, which results in e-mail systems everywhere being bogged down trying to deliver the unnecessary warning.

The responsible thing to do, if you receive such a message, is to go to the websites of virus checking software companies—such as [Norton](http://www.norton.com) and [McAfee](http://www.mcafee.com)—or the companies mentioned in the e-mail (in this case, you would check [Microsoft](http://www.microsoft.com) and [IBM](http://www.ibm.com)), and see for yourself whether the warning is true. (Every time I have received such a message, there has been nothing on any website—Microsoft, IBM, Norton, McAfee—about the particular virus. In other words, I have never found one of these alerts to be true.) If you don't find anything about the virus, it's because there is no such virus, so do your part and don't forward such hoaxes to everyone you know. The writers of these hoaxes get great satisfaction out of seeing their message

spread around the globe. Don't be gullible! Going to www.snopes.com is a good place to see if a virus is true. You can also check to see if those other emails you read are real or not. You will be surprised how much we read on line is not true.

- **Backup information on a regular basis** — Pick and schedule and make it a daily or weekly habit. Ask yourself each time you save a document or pictures...“Will I be okay if something happened to my computer and I lost my data?” If the answer is “no”, make sure to save your data to a permanent storage device. (See next item for more details.) This is good to have if your hard drive fails too. There is really no way to predict when your hard drive will fail, just like you don't know when your car will break down next. The average life span of a hard drive is 3 to 5 years.
- **Backup information on permanent, removable data storage media**, such as CDs, DVDs or USB Memory sticks and store them in a cool, dry place — and in a safe location away from your computer. Business should consider off-site storage of backups. This will allow businesses to permanently safeguard files from the possibility of an email virus. External hard drives will also work but are not as stable as the items mentioned. If an external hard drive gets dropped or jarred you could loose all the data on that hard drive. Their life span is also the 3 - 5 yrs.
- **Do your windows up dates on a regular basis.** These up dates block viruses from coming in. Windows up date messages appear in small pop ups in the lower right corner of your screen. The safe way to do up dates is as follows: Open Internet Explorer, click on Tools go down to windows update the computer will go to the windows website for checking your computer for up dates. Click on the Custom and the computer will check for up dates and give you a message Install up dates or there are no up dates at this time. (Windows XP users do not install Internet Explorer 8 – uncheck this box if it shows up.)

All of these things, together, will lessen your chances of infection. Most of all just remember to use common sense!

www.ActionOneComputers.com



Thank you, for choosing Action One Computers

We are honored that you trust us with your computer.