

## Virus Infections

Just like the common cold, there is no absolute defense to computer viruses, all we can do is play it safe and make good decisions. You have heard it before, make sure your antivirus programs are up to date, and that you run scans regularly. Avoid suspicious emails, websites and files. Do not download anything from the internet unless you specifically initiated the download or are on a website that you truly trust.

Your system will periodically attempt to run various programs, usually pertaining to antivirus or program updates. 99.9% of installed program updates take place when the program is started. The best example is Adobe Reader. When you start Reader, it does a quick check to ensure that it is up to date, if it is not, it will ask you to update it. If you have not started Adobe reader (opened a PDF file) and it asks to update, you should be suspicious of it.

The easiest way to identify the authenticity of an update popup is to open the program itself and run the updates from there. You can usually find Update under the Help menu of most programs.

The next thing you should do is find the "update settings"; they will be located either within the Update function, as described above, or under tools/settings. Once you are aware of the Update schedule (Daily, Weekly, Program Start, etc.), you will know when to expect the popup.

The real HP Update:

By default, HP update will run approx. once per month. There are currently no known fakes that look identical. If you see something very different, or do not have an HP computer, be careful.



## Microsoft Security Center

The security center is a built-in tool of the Microsoft Operating System; its function is to notify you of your Firewall, System Updates and Antivirus Protection Statuses. Virus developers have chosen to mimic this tool, many have done so very successfully.

Which is real?



I am sure that you notice a few subtle differences, but the fact of the matter is that it is not important which is real! What we want to know is how did these programs start up? Did you initiate it from within the control panel? Or from the Administrative tools section in the start menu? How about from within the Firewall settings, Windows Update settings or Windows Help tool? Was it by clicking the red warning symbol in the bottom right hand corner? If not, chances are that what you are seeing is a fake. Don't click on it!

Security Center will NEVER start on its own!!!

Antivirus Programs CANNOT start it either!!!

### **Antivirus Program**

It is very unlikely for your installed and up to date antivirus program to all of a sudden find many security threats. A properly installed and configured antivirus program watches your computer in real time. This means that every file you download from the internet, email you receive, file copied from a flash drive etc. will be scanned as it is written to your computer. This will trigger an immediate response and your antivirus program will report it immediately.

The notification will almost always be in the form of a small bubble style popup in the bottom right hand corner. Most will offer options to Remove, Delete, Quarantine or Ignore. Ignore is a very good indication that you are looking at a real antivirus program – but a bad idea to choose. Also look for specific file information and/or a “More Details” button. Finally, even the free antivirus programs that want you to purchase an upgrade, will not advertise on the security threat popup in the bottom right hand corner.

If you are not sure what to do or if you do not want to risk clicking on the popup, don't! Your antivirus program will prevent dangerous files from running for a short time - as long as you stop anything you are doing that may have caused it! If you were running a CD when the popup occurred, eject it immediately. Checking email, close it, and so on. Most importantly, if you copied/downloaded any files do not open them. Now open your antivirus program as you usually would, make sure it is up to date and run a Full, Thorough scan of your computer. The threat should be found again and now you know it is real.

### **Know your Machine**

The number one tool in defense of the computer virus is to know your machine. I know many do not like the idea, but the same rule applies to your car. It is not necessary to know all of the inner workings, but a basic knowledge of how to fill the fuel tank, what fuel to use, when to change the oil and how to ensure that your tires are filled properly is just as important to your car as Antivirus and Windows Updates are to your computer. Know your antivirus program and how it works and keep it and your system up to date.

Remember, the antivirus program industry is rather competitive; none of them will install other software for you! So, if you have Microsoft Security Essentials installed, only it will give you security warnings. The same goes for Avast, AVG, Norton, ESOT, Avira, MalwareBytes, ASquared and so forth.