Tips To Help Avoid Viruses….

By A1 Computers And Service - 2012

1. Check your email. You should ***never click on any link or attachment*** in an email unless you are certain that it has come from a trusted source. You need to remember that ***anybody's system can become infected with a virus***. So don't automatically assume that any message from your friend is safe. If the email message sounds strange, doesn't quite sound like your friend talking, then a quick phone call or reply email is all it takes to double-check that the message is really from them before you open or save any attachment. We need to ***pay close attention to any and all attachments received***. If you are not expecting something with an attachment do not automatically open it, ***even if it's from your mother***, best friend, or boss. Check with whoever sent the massage to be sure that they meant to send you an attachment. Also remember any attachment with a ***double extensions***, like .jpg.exe or .zip.vbs, are not what they might seem -- do not open them under any circumstances. (i.e.… Jane's 1st dance.jpg.exe).

2. Change your e-mail program. If you are still using ***Microsoft Outlook*** it is an efficient email program packed with many useful features, but the program is a ***frequent target of virus and spyware*** infections. There are free alternatives you can use such as ***Mozilla Thunderbird, Pegasus or Eudora***. To avoid using an email client completely you could use ***Gmail*** exclusively. If you still want to or have to use Outlook there are some anti-spam programs available that can help to cut down on spam and keep garbage out of you inbox.

3. Get a good anti-virus program. While this might seem obvious to some there are still many people who do not ***use a modern and up to date anti-virus program***. So the best way to avoid a virus is to set up your computer with a good anti-virus program then use it and keep it up to date. Programs like ***Avast, AVG*** or ***Avira*** are all ***great free options*** and do a very good job of scanning your system and keeping it clean. They can also set up to update definitions and scan your entire system on a regular schedule. While your anti-virus program is an area you do not want to skimp on and we are constantly being told that you get what you pay for, ***don't automatically dismiss any of the free options***. Any of the listed ones are as good as the higher-priced competition minus a few of the bells and whistles you may not need anyway.

4. Get a good anti-spyware program. Some would think that an anti-virus program and an anti-spyware application are the same thing, which would be wrong. The two programs are very different. They each look for different things, and even though their findings may overlap on some things, a good anti-spyware program will pick and detect things that the anti-virus program has missed. Some of the better ***free*** programs are ***Malwarebytes Anti-Malware***, and ***Super Antispyware***.

5. Use caution while browsing. The most common way your computer becomes infected is while you browse the internet, so keep an eye out for ***random popups*** that appear while browsing. If something shows up unexpectedly ***claiming to be your anti-virus*** software and reporting that your computer has problems or a virus, it's ***probably a scam***. Look carefully, and ignore anything with spelling errors or incorrect English or that refers to a program you do not have installed on your machine. Another scam involves ***popup advertising that warns of errors*** that can only be fixed if you purchase a particular brand of software. Obviously this is a hoax, and the software itself is likely to be a virus or piece of malware itself. If you encounter one of these, the safest thing is to ***close your internet browser immediately*** (do *not* click on the "scan" or "exit" buttons, and even the "x" to close the popup may trigger its nasty payload). The best way to close your browser is by pressing the ***CTRL & W key***. That will close any open window without you having to click on anything. After you close your browser it's a good idea to do an ***update your anti-virus software and perform a full scan***. It's unlikely that anything is lurking on your system, but it's a very good idea to check anyway.

6. Update everything. Configure your operating system to ***automatically download and install all of the current updates*** to your operating system, as well as any other patches or upgrades. This means your operating system will be kept in tip-top shape, making it less vulnerable to virus, spyware and security attacks. ***Check your other important system programs for updates as well***. Some of the more important to check for updates are Adobe Flash, Reader, and Shockwave. Also check the Java is up to date.

7. Use a different browser. Microsoft ***Internet Explorer isn't the safest browser*** on the market and it is a favorite target for malware and virus authors. There are ***better and safer alternatives*** such as ***Mozilla Firefox, Opera, Chrome, and Safari.*** These are seen to be faster, more flexible, and safer than Internet Explorer. ***Switching is easy*** (you can even import your bookmarks.). While it will be an adjustment when you start using the new browser pretty soon you ***won't even miss Internet Explorer*** at all.

8. Use a different operating system. While Windows is a good overall operating system and by far the most popular there are ***other alternatives that are much safer***. Linux has come a long way in being more friendly and usable to the average user. Some of the more popular distributions are ***Ubuntu***, ***Mint***, and ***Zorin***. These are all a ***free, safe and viable alternative to using Windows***. There will be a learning curve when you switch but the cost along with the ***better security*** is a very strong point to using these.

9. Beware of human error. Even using a more secure browser or operating system, ***human error can still lead to infections***. If an alert window interrupts and pops up while you're browsing asking if you would like to allow an automatic installation, ***break the temptation to click "Install" immediately*** and take a moment to review what's being asked. If in doubt close the browser (CTRL & W). Certain parts of the internet are more prone to viruses and nasty programs than others. ***Buying legitimate software*** from authorized sites is by far the ***safest and wisest option***. Trying to bypass security or save a few bucks by ***downloading pirated versions will almost always bring with it viruses and malware***.

10. Back up all of your data. Set up your computer to ***back up your files frequently and regularly***. If you're on the machine a lot, then once a day is sensible. If you aren't on your computer every waking hour then once a week should be sufficient. This way, even if a virus does infect your computer, you should be able to restore most (if not all) of your settings and data, with minimal document loss in the process.

Be alert, not alarmed. Use your common sense and don't freak out about the perceived threat of viruses and spyware. Don't download anything that looks strange. Don't click any links that seem not quite right. Don't open attachments that are unexpected or unusual. Scan everything -- twice, if you're skeptical. Update everything. Back up everything. And above all, you are your best defense, use common sense.