How to Keep Your Computer Healthy and Yourself Sane

Copyright © 2012 Adrian Hlynka – The Computer Doctor of Groton

The Internet is like the Wild West, exciting and full of opportunity – but also full of dangers that may not kill *you*, but will kill your computer and cost you a lot of money. Here are some important do's and don'ts to help keep your computer safe from evils that come from the Internet.

Of course the Computer Doctor can help you with all these things.

If You Use Your Computer for Business or College Work

Then it is worthwhile to take extra precautions to prevent computer problems that could affect your livelihood. There are five main things:

Backups

Your computer can go bad without warning at any time. In fact, the hard disk that holds all your data is the hardware part most likely to fail. So do backups frequently. The easiest backup tool is a miniature **USB flash drive**. These are tiny devices that can fit on a keychain. Also called "thumb drives", "jump drives", "memory sticks". More about these later.

If Your Computer is More than 3 to 5 Years Old…

Then it is too old to use to earn your living or for serious college work. The internal components are not designed to survive longer than 5 years. They are obsolete at that point anyway.

According to a study by Pinheiro, Weber, and Barroso in 2007, there is a 1 in 60 chance of a hard disk failing in its first year, and about 1 in 12 per year after they are 2 or 3 years old. A disk has only a 2 in 3 chance of lasting 6 years.

Backups are essential if you care about your data.

Also, any 5 year old computer will be very slow compared to a new one

Don't Share Your Computer

If you use your computer for work or business, or college coursework, don't let your kids or guests use it. Trouble is practically guaranteed. Young kids will mess up your computer because they don't know what they are doing. Older kids will mess it up because they do know enough to be dangerous.

Computers are cheap enough and your work is worth protecting.

Watch for Warning Signs

Hardware and software components of computers do some self-diagnosis, and provide warnings of some kinds of failures. Unfortunately, we are used to seeing warnings all the time, so it takes skill to know what to pay attention to. The computer doctor can check to see if your computer has been crying for help in its own language.

Use Appropriate Security Software

A commercial "Internet Security" suite of software that is configured and updated regularly is our protection against viruses, spyware, malware, and spam. It's not perfect, but it will stop most attacks. Those are far more likely to damage your computer than normal hardware failures.

Spyware and Adware – The Plague of the Decade

The biggest threat to your computer's health today is not viruses. It is software that installs itself on your computer without your knowledge. It hijacks your computer for its own purposes. Also called malware, it is parasite software that funnels advertising to your computer, or tracks your activities, or spies on you. Malware is more of a threat than viruses because people get paid to do it, and it is much more common. Sometimes well-known, reputable companies inadvertently promote malware.

A little malware on your computer may not be a big problem, but you will see advertisements you do not expect or want, and it will slow down your Internet activities. Some malware has criminal intent, to steal passwords and credit card numbers, etc.

A malware infestation will slow down your computer, even when off the Internet, and can even cause it to crash because the parasites may fight for control of your computer. Not surprisingly, they are not the best quality software and many of them contain bugs (defects) that cause unintended damage.

In bad cases of infestation, the damage is can be so serious that your hard disk needs to be wiped clean and all your software reinstalled. The hardware will not be damaged, but cleaning and reinstalling everything is very time-consuming and expensive.

Phishing

This is what it is called when a person or software tries to get you to give up information or money by official-seeming warnings. An email may masquerade as being from your bank or credit card company, and ask for passwords "to revalidate your account", for example.

What to Do About Spyware, Adware and Phishing

- ❑ **Never download or install any software, games, "plug-ins", or "add-ons"** except when recommended by knowledgeable and reputable sources. Free software sometimes comes with a hidden price.
- ❑ **Don't fall for pop-up ads that claim to fix your computer,** especially the scary-seeming ones. Free games and offers that claim to "enhance" your Internet experience or make searching easier are usually full of parasites, but so are some innocent-looking things. Especially things that claim to stop pop-up ads! Free music, file sharing, and game programs are usually infested with malware.
- ❑ **Don't fall for pop-up messages that warn that your computer may be infected.** This is a form of Phishing. Unless it is a message from software that you know is supposed to be on your computer, these warning messages are invitations to infect your computer. Sometimes after infection they will send "ransom" messages. They ask for money to "disinfect" your computer.
- ❑ **Buy and Use a good Internet Security Software Suite.** I use and recommend **Kaspersky Internet Security**. *Internet Security* is the name the industry gives to a package of anti-virus, firewall, anti-spam, anti-malware, and parental control software.
- ❑ **Run the Internet Security Software once a week**. (Or more if the computer gets very heavy use.) Make sure it downloads its updates, then run a scan and follow the instructions.
- ❑ **If you don't have good commercial Internet Security Software, download, install, and run Ad-Aware** (www.lavasoft.com) and **Spybot-Search & Destroy** (www.safer-networking.org) or ask the Computer Doctor to do it for you. Ad-Aware Personal and Spybot are free for non-commercial use.

E-Mail and Spam

Way too much e-mail is Spam (unwanted junk) these days. It clutters up our in-boxes. But it also is deceptive and potentially dangerous.

- ❑ **If you think an e-mail is Spam, just delete it without opening.**
- ❑ **Never buy something from a Spam advertiser, even if you actually want the item**. If everybody refused, Spam would die out.
- ❑ **Never click on a web-link in any e-mail.** This is often "phishing" in which these links take you to web sites that are convincing counterfeits of reputable sites. They try to trick you into giving up credit card numbers, etc. All of these are frauds because reputable companies are careful not to use low-security links like these.
- ❑ **Never open any e-mail attachment, unless you know what it is.** (A photo jpg from a family member is probably fine, but not much else is safe.)
- ❑ **Never act on any e-mail instructions to fix your computer or protect it against a threat.** Reputable senders will never send such messages.
- ❑ **Use a spam blocker, if you can find one that works well with your e-mail system.** Watch out, some spam blockers are too aggressive, and block good e-mails, too.
- ❑ **Watch for lost good e-mails**. Nearly every e-mail service now includes some built-in spam blocking, and many of them sometimes block good e-mails. This can sometimes be adjusted so they will not block e-mails you want.
- ❑ **Watch for lost blocked** e-mails that you send. Often legitimate e-mail messages are blocked by aggressive spam filters. Sometimes you as the sender get a message saying it was blocked. Sometimes not, so don't assume an e-mail got through.

Viruses

Yes, they are still a problem. Every computer needs anti-virus software, as part of an "Internet Security" Suite, or by itself. Anti-virus software needs daily or weekly updates to fight new viruses.

Be Careful When Installing New Software

You already know not to download or install random software. But even reputable software can slow down or clog up your computer, and make it start up very slowly.

Many software packages have a component that runs all the time, wasting your computer's time and memory. Often the software is "phoning home" to its maker's website, looking for updates (usually free) or upgrades (for money). Checking for updates every month or two should be good enough. Sometimes this behavior can be turned off.

Some software packages, especially ones for instant messaging, start up automatically every time you start your computer, which is wasteful unless you really do use them all of the time.

Cookies

Cookies are little data files that many web sites put on your computer. They are not a threat by themselves so don't worry about them. They have a valid use, **keeping track of your preferences on certain websites that you visit frequently**. Spyware parasites may take advantage of cookies to steal your information, however.

Windows Update

Microsoft took a lot of heat for bugs and security flaws in Windows. As a result they offer "patches," fixes and updates. Windows actually has a good procedure for updating your operating system.

- ❑ **Find the menu item called *Windows Update*, and click it.** Every month is probably often enough. The Windows Update website will guide you through the process. Some or all of this can be automated. You may be offered the choice of just critical updates, or other less important ones. Just take the critical ones unless you know what you are doing.

Backup Your Data – USB Drives

Even if you take all precautions, your computer can go bad without warning. A virus or parasite could infest and damage your computer before the scanners can detect the threat. Scanners can only protect you from things they can recognize. A lightning strike or even a simple power outage can destroy some of the data on your disk. Your kids or pets may mess up your computer. And of course computer hardware can just break down. Often there is no warning.

It is usually possible to recover data from a broken computer, but *not always,* and it can be very expensive, up to several thousand dollars.

A backup system outside your computer is the only good defense. How often, and what data, depends entirely on how you use your computer. Like gambling, never leave any data unbacked-up that you can't afford to lose.

The easiest backup tool is a miniature **USB flash drive**. These are tiny devices that can fit on a keychain. Also called "thumb drives", "jump drives", "memory sticks". They have made CD-ROMs and DVDs obsolete for backup use. You plug them into a USB socket and they appear as a new disk drive. You just drag and drop data to or from the drive. They have no moving parts and you can read and write them hundreds of times or more. Depending on capacity, they cost $10 to $75. Look for ones of 2 GB (the cheapest) and larger. Note that 2GB is three times the size of a CD-ROM.

USB devices can be installed or removed without turning off your computer. (This is called hot swapping.)

For huge amounts of data, use an **external hard drive**. This is a hard disk just like the one in the computer, in a portable case that plugs in to a USB socket. Not surprisingly, it appears as a new disk drive, just like a USB keychain drive, only bigger. Be aware that copying many gigabytes of data can take a long time. External hard drives are available in the 1000 GB size at reasonable price.

All other methods of backup are obsolete. Especially floppy disks, "Zip Disks" and all forms of tapes. CD-ROMs and DVDs are still good for transporting data when you don't want it back. They are much cheaper than USB flash drives.

Slow USB

Computers before about 2006 had USB 1.1 instead of USB 2.0. Or they may have had some sockets of each. This old kind of USB is 40 times slower than USB 2.0, which makes it useless for data backup. Now there is USB 3, which is supposed to be 10 times faster than USB 2.0.

Spreading the Risk

Parasite writers and hackers target the software that has the dominant market share. That makes sense. So running Microsoft **Internet Explorer** makes you more vulnerable than using **Firefox,** or another non-Microsoft browser. Some web sites used to work well only with Microsoft Internet Explorer, but that is not so true anymore with the latest versions of Firefox, Google Chrome, and others.

The same reasoning applies to Office Suites and e-mail client software.

That's Not All

This paper is about your computer's health. The Internet has other threats, of course, including fraud, ripoffs, gambling, pornography, etc. Please watch out for those, too.