10 Commandments for Happy Windows Computer Owning

by Robert Spotswood

How to reduce your computer headaches

I work as a computer tech and I see lots of different computer problems. But I see certain problems again and again. While it means more business for me, lots of those problems could be easily avoided saving my customers money and aggravation. Here are ten commandments, which, if followed, will greatly reduce your computer headaches.

I. Use a Virus Scanner

Get one and keep it up to date. The brand doesn't make a big difference. Keeping it up to date does! A virus scanner that has not been updated recently (recently being about 1 or 2 days), is only slightly better than no virus scanner at all.

Keep the virus scanner active and do regular scans of your system. Trying to install a virus scanner after you already have a virus infection usually isn't going to do any good. If the viruses are active, most will attack any virus scanner and prevent it from working or installing properly. The only way to stop this is to have an up-to-date virus scanner active when the virus first tries to infect you.

II. Protect Yourself from Spyware

Viruses aren't your only threat. Spyware is another, and virus scanners do almost nothing about it, although that is just starting to change. Spyware, aside from invading your privacy, can crash your computer, make it run slow, hijack your browser (especially Internet Explorer), annoy you with pop-up ads, and download porn. These things have cost people jobs and ruined relationships (see http://www.wired.com/news/infostructure/0,1377,63391,00.html).

Spyware can come in with other "free" programs, or can be installed silently if you use Internet Explorer (termed drive-by-downloading). If a window pops up asking to install software, say no, unless you were expecting it. While not all "free" programs are bad, avoid "free" programs without checking them out first. As a general rule, open source programs are unlikely to have spyware.

Don't use Internet Explorer (use Firefox or Opera instead), and check for "little pests" regularly. Spybot and Ad-aware are two free and good programs for dealing with spyware. Microsoft has also put out a free scanner

(http://www.microsoft.com/athome/security/spyware/software/default.mspx), although the default settings need to be changed (MS downgraded many threats to ignore by default). Unfortunately, it requires Windows 2000 and up, leaving 95/98/ME users to seek another tool.

Since there is no one scanner that can catch everything, you need to run at least 2, preferably 3, spyware scanners regularly. Beware of other spyware scanners, especially free ones. Most do a poor job, or are overpriced, or both (see also http://spywarewarrior.com/rogue_anti-spyware.htm). Spyware is getting nastier over time, and some is all but impossible to remove even for the experts. Prevention is the still best medicine, and in some cases the only medicine.

III. Don't Open Strange Emails

Never, ever open or respond to an email that in any way seems suspicious. Don't even preview it, especially in Outlook or Outlook Express. It doesn't matter who is appears to come from. That can be faked unless you use digital signatures correctly, and most modern worms do fake the sender.

Don't rely on your virus scanner to protect you either. Email viruses can spread around the world in minutes. Your virus scanner will be at least a day behind the most current threat.

No legitimate company will want you to open an attachment or enter your user info in a form from an out-of-the-blue email. Companies also do not send patches (see commandment VIII) via email. Should you actually find a company that does these things, find somebody else to do business with. Your information is not safe with them.

If at all possible, do not use a Microsoft email client. Use Thunderbird or Opera based program (among others) instead. Microsoft's poor security record AND actively being targeted make for a lousy combination.

IV. Never Respond to Spam

Never respond to or buy something from an email that you even THINK is spam or unsolicited, even if it's something you are interested in. Spammers spam because it is profitable. It is profitable because enough people buy or respond. Buying anything from or responding to spam is just throwing gasoline on a fire. In addition, often, the spam involves something either fraudulent or illegal. If it's something you are still interested in, do a web search, and buy from there.

Always be careful of where you put your email address. Putting your email address in some forms (paper or electronic) is one way the spammers get your address, especially contest promotions, i.e. fill out a form for a chance to win a prize and the form asks for an email address among other things. Posting your address on a website or Usenet are two other ways spammers get your address.

V. Perform Regular Backups

Sooner or later, it's going to happen. Something important gets deleted. It doesn't matter if it was a virus, equipment failure, or just not paying enough attention when hitting the delete key. This includes not just erasing files, but overwriting data. The recycle bin or undelete programs can't help you then. Doing proper backups are your best, and cheapest defense against these disasters.

Take care of your backup media. Don't leave CD's lying in the sun or tapes near magnets. Finally, don't forget to test the restore process once in a while! A backup you can't restore is worthless, and the practice you get in restoring will help you avoid mistakes and panic when the time comes to do it for real.

VI. Help the Tech

Having computer problems is normal. Sooner or later it happens to everyone. When it is time to seek help, don't lie. Chances are the tech will see through the lie very quickly, and even if he doesn't, it only makes it harder for him to help you. Be as specific as you can. Write down the exact error message. Tell him anything you think might be important. He can't read minds and he wasn't there when you did _____ (fill in the blank).

Don't "clean up" your computer before you bring in (or take the computer to) the tech. This can, in rare cases, disguise the cause of the problem.

If getting phone support, be in front of your computer, have it turned on and booted up, and have the application(s) already open (if appropriate). Many phone support techs are rated (and promoted or fired) based on how many calls per hour they answer, not on whether they actually help you. Take too long and you may find your problem is "We do not support that. Goodbye." Be patient and describe everything you see. Phone support is one of the hardest types of support to do.

Finally, swearing like a sailor or threatening the tech will not get your system fixed any faster or cheaper. In fact, the reverse may happen.

VII. Get Some Computer Training

You don't have to be a mechanic to drive a car, but you still have to have training. No one is born knowing how to drive, and no one is born knowing how to use computers. Know the basic terminology, specs, and workings of your computer. This knowledge can reduce your need for professional help (aka the tech) and make working the tech more productive when you do need it.

Think of the training as an investment in yourself. Once you learn how to use your computer your [computer] life will become more productive and enjoyable. In Houston, HAL-PC is one of many places that offers a variety of free or low cost training. Take advantage of it.

VIII. Apply Patches Regularly

Programming is easy, but creating perfectly secure programs is very hard to impossible. Mistakes happen. When they do, fixes (often called patches) are issued. While some of these patches may cause problems, it is usually better to install the patch than not.

Free and open source software usually just issues new versions rather than patches, so don't forget to upgrade. There are mailing lists you can sign up for to tell you when new patches and new versions are issued.

Using Windows update regularly is a good way to stay current with your patches. Be warned, however, that Microsoft does not always issue patches in a timely manner, and neither do some other software companies. You can't patch without a patch.

Sometimes, a patch will not fix the problem it was intended to fix or may even open up other security holes. Do not make the mistake of thinking that just because you are current on all your patches that you are safe. You're not!

IX. Pay Attention to Your Computer's Security

The wrong types of people are interested in your computer, even if you are just a home user on dial-up. Even if you don't have any valuable data (unlikely; credit card info, banking info, perhaps work info are just a few examples), your machine could be used as a source of spam (most spam is sent this way nowadays), used to host illegal materials, or even as a launch pad for attacks on other systems. A dial-up user, or someone with a connected modem, could be disconnected from his ISP (Internet Service Provider) and silently reconnected to another overseas. The next phone bill will be quite shocking.

While there is no product that can make your computer secure, a firewall and virus scanner are a good start. Running more than one firewall and one virus scanner at the same time is usually a bad idea. It does little to increase your security, while greatly increasing problems you will have.

X. Give Your Computer Regular Maintenance

Computers, like all things, work better if they receive occasion maintenance. A scandisk and defrag every month will help keep your computer running smoothly. Dusting inside your computer every so often is also a good idea. Seek professional help if you are unsure how to do this. Smaller computer shops will often teach you how to do this yourself for free or a small fee or you could make a friend with a PC tech. Finally, your computer case is not a refrigerator door. Don't stick magnets on it.