[Originally published in What Where When Magazine (Baltimore, MD), October 2009; Volume 25, Issue 3]

An Oil Change for Your Computer
by Yakov Shafranovich

Hardly a week goes by without a phone call from some unfortunate person whose computer suddenly assumed a mind of its own and is no longer the useful tool it used to be. Most of the time it turns out to be a virus of some sort. At the end of the repair, I usually give them a short pep talk which starts like this: A computer is like a car; just as a car needs an oil change, so does your computer....” In this article, I will summarize some of the important points of this pep talk in this article in hopes that it will be useful for others.

Why Do Viruses Happen?

Computer viruses are almost as old as computers. However, they really gained effectiveness with the rise of the internet, which allows them to be spread faster and much more easily. Internet worms have been known to infect hundreds of thousands of computers in less than a day. When your computer starts being very slow, and random advertising pop-ups appear, even though no one is using the computer, it is usually a sign of some sort of a virus or spyware, albeit not always. The slowness is caused by the viruses consuming resources on your computer. Pop-ups are how they make money.

The question most people wonder is what lets these things happen in the first place. Because of the tremendous complexity involved in writing software, many software programs have numerous security holes, which viruses utilize to make their way into unprotected machines. Security holes are often mistakes made by the original programmers, who never considered the security implications of what they were doing, or simply loopholes found by hackers. To close these security holes, software vendors release updates or “patches” on a regular basis. However, it remains an ongoing race between the “bad guys” seeking to exploit these vulnerabilities and the vendors trying to patch them before they become widespread. In a way, computers are like castles with the barbarians at the gate and the software vendors scrambling to plug the holes.

Even on fully secured computers, viruses can make it in when users think they are installing something useful. An enticing email offering, some free tool, or a free computer game often fools computer users into downloading and installing malicious software. These viruses are known as “trojan horses.” While anti-virus software may catch some of these, no amount of technology can completely protect against people installing viruses by mistake. The rule of thumb is that if something is too good to be true, it probably isn't. So if a website is offering a program for free, you must make sure the company is legitimate, either by using a trusted source, such as Download.com, or checking with the Better Business Bureau (www.bbb.org).

Another question I am often asked is why are viruses, trojans, etc. written in the first place? What do their authors gain? The answer is very simple – money! There is an entire underground economy on the internet involving people who write viruses, those who distribute them, and those who use them. Viruses writers and distributors often get paid 10 to 50 cents for each computer they infect. The infected computers, which are banded together into large networks known as “bot nets,” are used to send spam, host illegal content and pornography, provide untraceable ways for hackers to attach other computers, and serve ads. The more nefarious kinds of viruses may encrypt your data and hold it hostage until you pay. They can watch your online banking, providing hackers access to your bank account, or in the worst cases, they can be used for identify theft or corporate espionage. All of this generates billions of dollars yearly for the bad guys.

Update Early, Update Often

The first line of defense against viruses is to keep all of the software on your computer up to date. The basic software that operates the computer is known as the “operating system.” The most widely used operating system is Windows, currently either Windows XP or Vista. A minority of users use Mac OS or Linux. For all of these, applying updates released by the vendor is absolutely essential. According to the SANS Institute, an average Windows system that is not kept up to date can be infected in less than 30 minutes. Ignoring updates is the number one way to make sure your computer plays host to some nasty critter. Keep in mind, as well, that older software stop being supported by vendors at some point. If you are running an operating system that is more than 10 years old, it might be prudent to look into upgrading.

Patches for most operating systems are released on a monthly basis. Microsoft releases updates for Windows on the second Tuesday of every month, known in the computer world as “Black Tuesday.” For Windows computers that are connected to the internet, a small pop-up usually appears at the bottom right corner with a yellow shield indicating updates. It is important not to ignore it. If your computer for some reason fails to detect updates, you can easily remedy the problem by going to “Control Panel>System->Windows Updates” and selecting the first option to detect and install updates. On Windows Vista, this option is under “Control Panel>Windows Updates.” It might be a good idea to check your computer right now to see if that setting is set. If for some reason that does not help, you can visit Microsoft’s website to update your computer manually at http://windowsupdate.microsoft.com (make sure to use Internet Explorer). Mac OS and Linux provide similar update mechanisms.

In addition to system updates, any software that is used for browsing or email should be updated, since it can be used by an internet-based virus or hacker to enter your computer. On most computers, this includes the browser (Internet Explorer, Firefox, Safari, Opera, or Chrome), Adobe Flash Player (used for visual content), Apple Quick Time (used for video), Adobe Acrobat Reader (used for PDF files), Sun’s Java (used for visual content), and email software (Outlook, Thunderbird, etc). You don’t have to go to your computer and look for these – they will prompt you to update regularly. If you wish to update manually, most of these can be updated by going to “Help>Check for Updates” within each individual program.

It is also important to keep your word processing software up to date, since Microsoft Office files can be used to spread viruses. On Windows Vista, the update will happen together with Windows updates; on Windows XP you can set it up to do that automatically by going to update.microsoft.com. Microsoft Office for Mac OS has its own update mechanism, but you can update it manually by going to www.microsoft.com/mac/downloads.mspx.

Occasionally, an update may break some other program on your computer. If that happens, you should check with the vendor if they have a newer version that will work with the update. Otherwise, you can always uninstall a specific update by going to Control Panel>Add/Remove Programs” in Windows XP, or Control Panel>Programs and Features>Installed Updates” in Windows Vista. Be aware that updates are meant to protect your computer, and if you decide to take one off because some other program stopped working, the hole that the update was meant to patch remains open, thus leaving your computer vulnerable.

Immunizing Your Computer

The second line of defense for your computer is anti-virus software. It will protect you against viruses coming through unpatched security holes, but most important, it will protect you from human mistakes. It is extremely important to keep anti-virus software current and to update it frequently – daily, if not more often. New computers often come with a free 90-day or six-month trial of anti-virus software, which then expires. Expired anti-virus software will not update, thus leaving your computer vulnerable.

There are numerous free anti-virus programs that can do the job as well as the commercial products. Some examples are Avast (www.avast.com), AVG (free.avg.com), Avira (www.free-av.com), and Microsoft Security Essentials (www.microsoft.com/SECURITY_ESSENTIALS/). However, be aware that these come with minimum or no support, which may leave you stranded if you need help. You should also be careful that the free anti-virus you are getting is not in fact a virus by checking with a trusted source like the BBB (www.bbb.org) or Virus Bulletin (www.virusbtn.com). Free anti-virus products often come with higher-end, paid versions, which include support and extra functions, like a firewall.

Before installing free or commercial anti-virus software, you should spend a little time researching what professional publications say about that particular product. For business use, or for those who want support and peace of mind, commercial anti-virus software is cheap and widely available via stores like Staples and Office Depot, or online. (Free anti-virus product can only be used legally for personal use; businesses should use commercial products.)

People often have a second, older computer, without internet access, that they use just for word processing or computer games for the children. They assume that, since there is no internet on that computer, it is not vulnerable to viruses. That is not entirely true. While viruses do primarily travel via the internet, there are still some viruses that go the old fashioned way: via floppy disks, flash drives, and even Word files. So if you plan to share disks or flash drives with others, it is important to have an anti-virus installed on your computer. Most anti-virus programs allow you to download updates via a flash drive.

Firewalls and Alternative Browsers

Here are some additional tips to make your computer a little safer. A firewall protects your computer against random attacks from the outside. While the router you got from your internet provider has a built-in firewall, a software firewall will provide an extra layer of protection, and will protect you if you travel with your computer. Windows XP and Vista include a built-in firewall, called Windows Firewall. You can check to see if it is enabled by going to Control Panel>Windows Firewall. If your Windows XP computer does not seem to have one, please follow the procedure above for updating it to the latest version. Many anti-virus programs include a firewall as well. For the more technically inclined, you can also install a free firewall that is more advanced than plain Windows Firewall from www.zonealarm.com. Generally, when you install another product containing a firewall, the Windows Firewall will be automatically disabled.

Another popular security recommendation is to use an alternate browser. Since a browser is used to access web pages, it is usually the main entry point for viruses. Most Windows computers come with Internet Explorer as the default browser. But, because of the very tight coupling between Internet Explorer and Windows, it is less secure. The most widely recommended alternative is Mozilla Firefox, which can be downloaded for free from www.mozilla.com. Apple's Safari 4 (www.apple.com/safari/), Google Chrome (www.google.com/chrome/), and Opera 10 (www.opera.com) are other popular browsers that can be used instead of Internet Explorer. However, being that Internet Explorer is an integral part of Windows, it cannot be uninstalled. You can however, set one of the alternative browsers as the default browser for your computer by going to "Control Panel>Add/Remove Programs->Program
Access/Default Programs." As mentioned above, all of these also have vulnerabilities, to a lesser degree, and must be updated in a timely fashion.

Backup, Backup, Backup

The second most common problem that people approach me with is hard drive crashes. Because a computer's hard drive has moving parts and is constantly spinning at about 5,000 revolutions per minute, it is the part that breaks most often. Sometimes data from a crashed drive can be recovered, but often it cannot be without paying a large fee to a specialized service bureau. This is why it is important to perform frequent backups of your data.

Until recently, most backups were done onto a CD, external hard drive, or flash drive. The problem with these approaches is that in cases of a fire or a lost laptop, the backup is usually gone as well. Additionally, flash drives lose data very easily by simply being unplugged while in use. Metal detectors and other magnetic devices have been known to wipe out flash drives as well. The main issue with backups, however, is that simply they are a hassle to do, and most people don't remember, or don't bother, to do them.

Thankfully, there is an easy solution – online backup. Online backup programs run in the background on your computer, silently backing up your files on a regular basis. It is no bother for you, and also assures that your data is safe hundreds of miles away. You can download and install a free online backup program for up to 2GB of data from Mozy (www.mozy.com). If you need more than that, both Mozy and its competitor Carbonite (www.carbonite.com) provide unlimited online backup for less than five dollars per month. For Mac and Linux users, as well as more technical Windows users, there is also JungleDisk (www.jungledisk.com), which costs about $2/month (plus data storage fees).

One drawback of online backup software is that, while these companies claim that your data are secure, there is always a possibility of a hacker getting in. Mozy is owned by EMC Corp, a Fortune 500 company. JungleDisk is owned by RackSpace, a public company, and uses a storage product from Amazon.com, also a major company. These companies have a lot at stake, so they tend to secure their products well. Most online backup software will encrypt your data before it leaves your computer, which protects it during transfer, but does not protect it once it lands on their servers. Some, like Mozy and JungleDisk, offer the option of setting a special password and encryption key on your data so it remains encrypted on their servers. This provides a peace of mind for users, but if you forget your password, your data will be lost.

My hope is that this simple article will help people understand how to keep their computers safe.

Comments and suggestions are welcome via email to yakov@shaftek.org.