

Protecting your PC from the digital world

If someone asked me what two things I heavily use everyday they would be my laptop and truck.

Most everyone relies on their automobile and personal computer for transportation and communication. It's hard to imagine what we would do without gasoline and electricity.

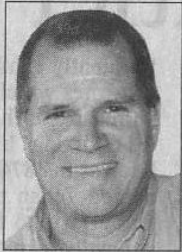
With the environmentalists restricting oil exploration and the Islamic fundamentalists targeting our power grid we may find out one of these days.

As long as there's money for the soon-to-come \$5 a gallon gas and the juice stays flowing, I'll keep driving to work on computers for a living. One big difference between my truck and my PC is the maintenance and effort to keep them running properly.

About once a month I change the oil in my truck and once a year I take it in for a tune-up. My computer is a different story since it requires updates and fixes almost on a daily basis.

Can you imagine what a pain it would be if you had to work on your car or truck every day?

These constant updates include antivirus definitions, antispyware threat additions, anti-spam source lists and



John Deans

Microsoft Windows updates and service packs. Our computers need these critical updates due to the fact that they are under constant attack from hostile external forces from the digital world.

If I had a computer that was never connected to the Internet or ever had a CDROM or flash thumb drive inserted into it, there would be no need for all those updates. It would sort of be like never having to change the oil in my truck if I never drove it.

Since so many resources are Web-based, it is almost useless to have a computer that is not connected to the Internet.

Basically if you have an automobile you drive it on the road with other cars, just like if you have a PC, it communicates with other computers on the Web. The problem is that PCs are higher maintenance than cars.

As I said before, the antivirus and antispyware programs are hard coded to check on a daily if not an hourly basis for new updates, lists and definitions to stay ahead of the threats. This is like a cop assigned to protect your home that gets a constant stream of bad guy photos.

A more proactive way to fight the threat is to harden the Window's operating system (OS) to eliminate the vulnerabilities. This is like locking up

the doors and windows in your home to make it more difficult for the thieves to enter.

That is what the Windows Update utility performs by downloading and applying the most up-to-date fixes and patches that bad guys exploit to gain access to your computer.

Windows Update was introduced with Windows 98 and has gone through numerous modifications and revisions since then. With Windows ME Microsoft released Automatic Updates which allowed the user to schedule the download and implementation of the updates.

This capability is not limited to just personal computers since Microsoft also rolled out Software Update Services with Windows Server 2000 which was the prominent OS for servers at the turn of the century.

Though the number of wide spread attacks from viruses and hackers have decreased over the past few years the threat is still out there. However, the hundreds of patches to Windows over the years has made much more difficult for the bad guys to penetrate our computers.

When I first started my consulting business here I made many client site visits to manually run the Windows Update utility to make sure their PCs were protected with the latest updates.

However, I was hesitant to put them on Automatic Updates since in the early years there had been numerous bad updates that messed up Windows or caused some weird performance behaviors.

Over the past couple of years I have converted the vast majority of my client PCs to utilize the Automatic Updates since those early Windows Update problems have been resolved. Still, from time to time I will get hit with a Microsoft Update patch problem that messes something up on a client computer.

At this time the benefit and protection that the Automatic Updates provides far outweighs the rare risk of problems.

Windows Update is manually run on Windows XP within Internet Explorer (IE) by clicking on Tool-Windows Update. This takes you to www.update.microsoft.com and starts the process of evaluating your version of Windows, the revision of Windows Update, and the list of fixes and patches already installed compared to the ones that are available at that time.

Before the actual updates are applied for the first time, Windows Update will most likely have to update itself with the latest version. After it verifies the installation of Windows is in fact a legal copy, it will then download and install the most recent version of the Windows Update application.

Basically you just take all the defaults

at the prompts and let it do its thing. I recommend just installing the critical security updates which are the most important ones to get implemented.

Service packs are just large groups of patches and fixes that are downloaded in a single large file that could be over 100 MB and take close to an hour to install. Just recently the latest service pack for XP has been released called Windows XP Service Pack 3. I keep this on my flash drive for quick installations at my client sites. Other service packs I have on that 8GB thumb drive are Office Service Pack 3, Vista Service Pack 1, and Windows Server 2003 Service Pack 2.

Windows Vista now has a control panel utility for the Windows update application and it also has the automatic option enabled by default. In fact, many times a year Microsoft will reboot your computer after critical updates are applied.

That still bugs me that Bill Gates can reboot my PC whenever he wants...

Bottom line: Windows Update is a critical tool that needs to be utilized to protect our PCs from the ghouls of the digital world.

Next week's column: Made in China.

John Deans of DeansConsulting.com is a Brenham area computer networking consultant who can be reached at 289-2233 or John@DeansConsulting.com for questions and comments.