KEEPING WINDOWS CLEAN

Windows is a living entity. Protecting Windows and keeping it clean from malware (malicious programs) is a full time job these days. Windows users are often frustrated by Microsoft's continued efforts to make its operating system secure against hackers because patching Windows seems like a full-time job. The real question here is what do all these patches mean to you? Microsoft releases "critical" alerts on a regular basis designed to protect Windows from hacker attacks. The most severe vulnerabilities deal with security bugs that allow hackers to gain complete control over your computer. Some of these flaws exist in the way Windows Media Player and MSN Messenger process certain files. Microsoft has also identified bugs in how Exchange (its Internet Mail Server Software) and Office allow hackers to execute hostile code on vulnerable systems. These patches are supposed to prevent a hacker from gaining unauthorized access to certain sections of a Web site. Another bug in the Windows Shell Component may permit a hacker to cause an affected system to stop responding. These vulnerabilities make it possible for hackers to spy on your PC. With the advent of Service Pack 2, it seems like updates are a seamless process that simply execute in the background. The problem with this "easy" method of installation is that you, as the user, need to know what is being changed on your computer. This is why I recommend you always view the list of updates before allowing Windows to update your system.

Security Updates

One Microsoft security patch update includes a change to the functionality of a clear-text authentication feature of Internet Explorer. This update removes the ability to handle user names and passwords in HTTP URLs, HTTP with Secure Sockets Layer (SSL), URLs, and HTTPS URLs. An example of the type of URL that is no longer supported would look like: http(s):// username:password@server.com If you think your version of Windows is too old to be affected by these security concerns, think again. Windows 98, Windows 98 SE, and Windows Millennium Edition are all critically affected by these security vulnerabilities too. If you are running Windows NT 4.0 Workstation SP6a or Windows 2000 Service Pack 2, update support ceased at the end of last year. Microsoft encourages those users to migrate to a "supported" version of Windows to prevent potential exposure to these security vulnerabilities.

Protection Settings

You can take steps to protect yourself from future attacks. Set your Internet and local intranet security zone settings to “high” so your computer will prompt you before running ActiveX controls and active scripting in these zones. Setting your browser security to “high” applies the highest level of protection from unsafe content that comes across your network. If this setting causes some of your sites not to load properly, you can add those sites individually to your list of trusted sites. However, you should only do so if you are sure that the site is safe to use and is hosted from a company or entity you trust. As a final note, there is a free program that I highly recommend you download called the “Microsoft Baseline Security Analyzer” (MBSA) tool that verifies when a security update has been applied to your system. It lets you scan your system for missing security updates as well as common security misconfigurations.

Firewalls

Once upon a time, a firewall was your best answer to protecting your computer from hackers looking to exploit vulnerabilities in Windows. Unfortunately, this isn’t always the case now. Nowadays, most users are attacked by just browsing the Web. Hackers host Web sites that contain code to exploit vulnerabilities in your operating system such as infect you with a virus, spyware, or even take complete control of your computer. Hackers can alternatively compromise a Web site for the purpose of misdirecting you to click on malicious content. Hackers can’t “force” you to visit a specific site, but they can trick you into clicking on a link that invites malicious content into your machine.

Windows XP SP2 has an integrated firewall, previously known as the Internet Connection Firewall (ICF) that defends you against hackers who are trying to access your computer from the Internet without your permission. When a hacker attempts to connect to your computer via an “unsolicited request,” the Windows firewall blocks that request. Windows will actually ask your permission if you wish to “unblock” and allow connects to programs you actually want to run such as instant messaging and multiplayer network games. When you unblock those connections, the Windows firewall creates an exception so that the firewall won’t ask any more when your program needs to receive information to function. You don’t have to use the Windows firewall. You can install and run any firewall you wish.

Zone Alarm is an excellent firewall that is very popular. Zone Alarm offers both paid and free versions that can protect your computer as much or as little as you desire. An even more comprehensive program is Norton Internet Security 2005 that touts its ability to hide your PC on the

Internet so hackers can't find it. The Mac also has an integrated firewall, just like Windows. However, Norton also makes a comprehensive security solution for this platform as well in the form of Norton Internet Security 3.0. The best part of Norton Internet Security 2005 for the PC is its integrated "Intrusion Detection System" that automatically blocks suspicious traffic. Not only does this product block suspicious incoming connections, but it lets you configure your "outbound" Internet connections too. This is advantageous, because if you do get infected with spyware, Norton will alert you that a program on your system is attempting to connect to the Internet and asks you if you really want this program to connect. By giving you the opportunity to block these connections, you can effectively thwart malicious spyware from doing its evil.

Intrusion Detection

Apple's Macintosh has its own version of this type of Intrusion Detection with a program called, "Little Snitch" that effectively asks your permission any time a program wants to connect to the Internet. Although the Mac seldom becomes infected with spyware, it is a handy utility to have so that you know exactly what your computer is doing on the Internet.

Frozen Images

Now that your computer has been through its trial by fire(wall), the best answer is to simply put your computer on ICE! If you have resigned yourself to the fact that, no matter what you do, your computer is going to get infected, then use a program called "Deep Freeze". This software for both Mac and PC lets you configure your computer with all the programs you need and then "freeze" your configuration. If a hacker infects your computer with a virus or spyware, Deep Freeze makes the damage simply disappear. All of your settings, files and programs are completely restored to their original configurations every time you restart your computer. This makes it possible for you to avoid problems caused by software conflicts, registry and operating system corruption, lost network and Internet connections, as well as a host of problems caused by simply connecting to virus-ridden network sites. The only catch is that you have to store your personal documents on a separate drive that does not "revert" each time you restart your machine. You have to imagine this program literally resets your computer to a frozen state that you specify. However, if you create a word document, it would be lost if it were on that drive. So, remember to keep a separate drive with your personal files and you'll have a computer that won't ever become infected or go down. Now, all you have to worry about are mechanical failures.

Conclusion

Finding ways to prevent hackers from accessing Windows is difficult because your operating system is always in a constant state of flux. Every time you turn on your computer, browse the web, or get a

Microsoft update, your operating system changes. If you want to prevent all changes from taking place on your computer, freeze the computer—but then you can't make any changes to your operating system at all.

There are good and bad points to both approaches—but in a world where having a functional computer is a necessity—this Tech Tip will keep your system running.

Source : http://www.geeks.com/techtips/2005/techtips-DEC08-05.htm