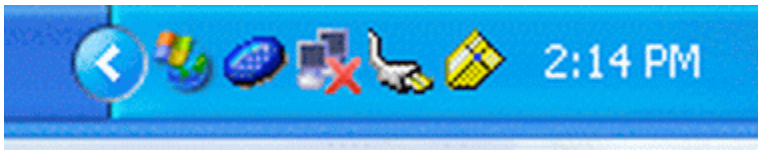
University of Tennessee at Chattanooga
ARCS, Michael Ward, 2005-7-27
Basic Windows Security

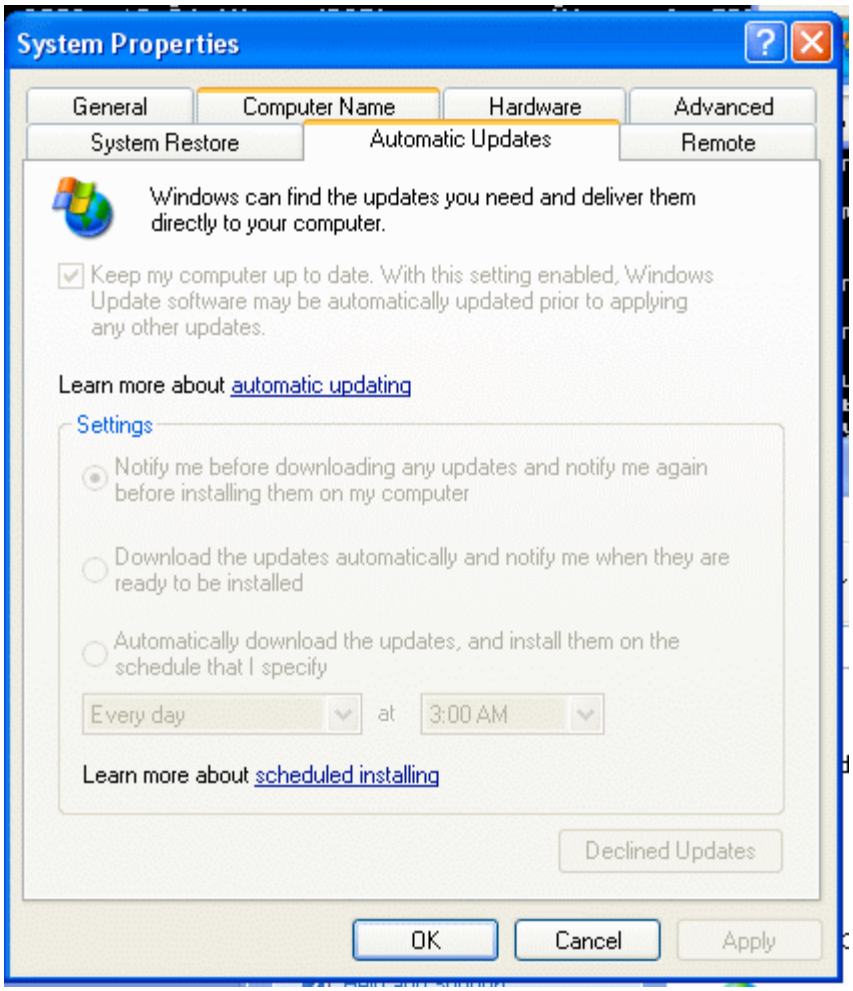
Nothing, besides turning off the power, can insure that your PC will be completely protected from hazards such as viruses, worms, and hackers. At UTC several layers of networking defense, including a firewall and vigilant networking administrators, help protect faculty and staff computers. While these measures provide a good medium of security, the most important factor in the security of your PC is you. The following are a few steps that can help ensure that your PC is secure.

Carefully consider opening ANY attachment. Modern viruses can forge the "From:" field, making it appear that an email originated from someone you know. Don't be fooled by the attachment's extension (.ZIP, .PIF, .SCR) into thinking that it will be safe to open, as viruses always arrive disguised as something else. If in doubt, delete it.

Keep your system up to date. Windows XP and Windows 2000 (with Service Pack 3 or greater) have an Automatic Updates feature that will download and install the latest patches from Microsoft. This feature has a unique icon that appears when you need to configure or update your system. Find your clock, usually its in the lower right corner, and look for a "Windows and World" icon.



In this picture, it is the icon second from the left. Double clicking on the icon will start the update dialog and provide instructions on what needs to be done. If you do not see this icon, it could be that your system is automatically configured to update without your intervention. This can be verified (Windows XP) by clicking Start->Control Panels->System->Automatic Updates.

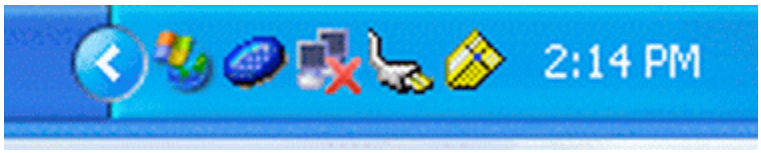


If "Settings" is grayed out, your system is set to automatically update. If you can configure "Settings," make sure to enable the first choice "Keep my computer up to date." For Windows 2000, click on Start->Control Panels and you should see "Automatic Updates." Double clicking will bring up a screen similar to the one for XP (see above.)

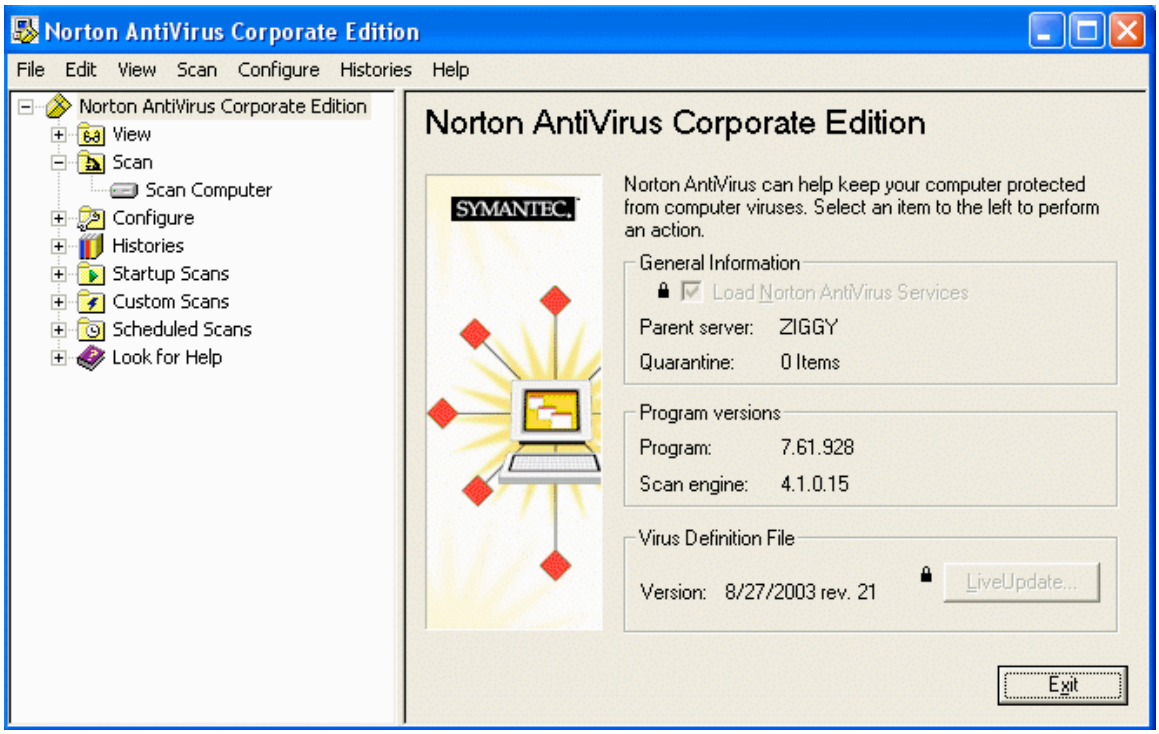
It is also possible to manually update your system by visiting:
http://update.microsoft.com/microsoftupdate

Microsoft has provided a means of having a "local" copy of the critical updates called Windows System Update Service (WSUS). ARCS has implemented a server for WSUS and directions for using it can be found at:
http://slug.ceca.utc.edu/windowsupdate

Make sure your Norton AntiVirus definitions are up to date. Again, looking near the clock you should see a "little gold shield." If you do not see this shield, you need to contact the Helpdesk (4000) for installation of Norton AntiVirus.



Here it is nearest the clock. By double-clicking on it, you will bring up



The "Virus Definition File" needs to be dated within two weeks of the current date or your system is out of date. UTC's Norton AntiVirus server "pushes" definitions out to every client as soon as they are available. If your definitions are out of date, you need to contact the Helpdesk (4000) to rectify the problem. Your home PCs should be protected as well. Two very good antivirus programs, both of which are free for personal use, are:

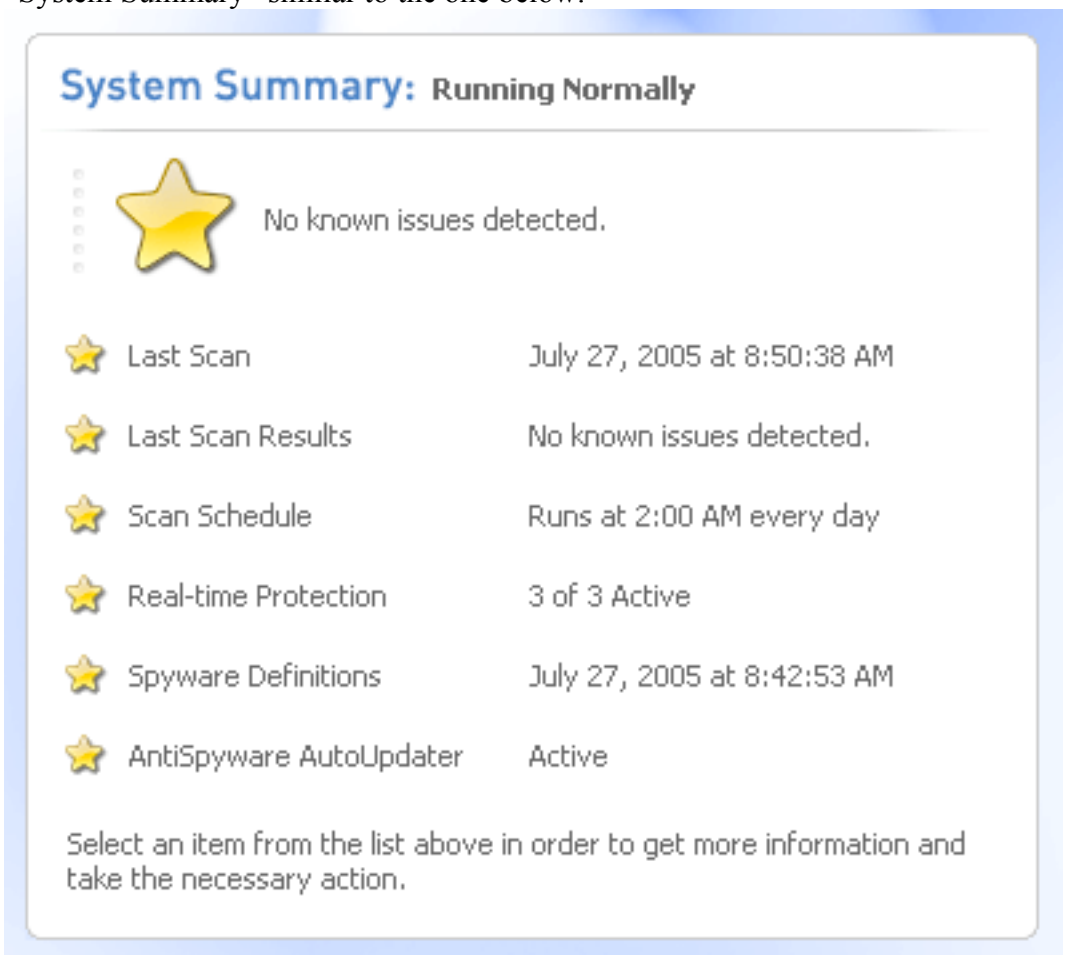
Antivir: http://www.free-av.com/
AVG: http://free.grisoft.com/doc/1

Please remember that your antivirus program is only as good as its last update.

Keeping your PC safe from Malware. Malware, which includes Adware and Spyware, is becoming a greater problem than viruses or SPAM. The activity of Malware programs can range from just monitoring your surfing habits and producing pop ups to stealing confidential information such as credit card numbers. Microsoft is helping users fight this problem with a product called Microsoft AntiSpyware. This product does the same job as antivirus programs, except it targets spyware. The Helpdesk can install this program or you can download it from:
http://www.microsoft.com/athome/security/spyware/software/default.mspx

When the program is active, Microsoft AntiSpyware is represented by a "target" icon within the system tray.

Double-clicking the target will bring up the main program. Optimally, you should see a "System Summary" similar to the one below:



Microsoft AntiSpyware also needs to be updated routinely or the protection it provides is severely limited. By default, the program will automatically update itself and perform daily scans for spyware.

Safe Surfing. Just like the real world, there are "dangerous" places on the Internet. Blindly surfing the Internet by clicking on any provided link can lead to a PC infested with viruses and malware. Don't click on popup ads "just to see where they lead." UTC computers should not be used to visit any site that involves pornography, online gambling, or any other questionable materials.

You can also improve your security while surfing by using the Firefox browser instead of Internet Explorer. While IE is considered the standard browsers for Windows users, it is also more prone to vulnerabilities. You can get Firefox from:
http://slug.ceca.utc.edu/

Avoid Peer 2 Peer. Grokster, eMule, and Kazza are just a few of the P2P file sharing applications that can be found on the Internet. While there are a few legitimate reasons for using such a program, the majority of users download copyrighted materials using P2P apps. Downloading such materials, including music and videos, is illegal. P2P applications are often bundled with malware such as spyware and adware, which gets installed with the P2P app.