

Connect

Information Technology at NYU

[Search This Site](#)**F a l l 2 0 0 3 E d i t i o n**

Browse the table of contents, or select an option from this menu:

[Computer Security Corner](#)[Print this article \(127K PDF\)](#)[Current Issue](#)[Archives](#)[About Connect](#)

Tips on Securing Your Windows Computer in Insecure Times

By **Tracey Losco**

It seems as though every time you turn on the radio or television these days you hear about a new computer worm or virus. Most of these programs target Windows machines—the most popular platform—and infections can spread quickly and cause a great deal of damage. This article outlines a few simple steps that every person running a Windows computer should take to protect his or her computer against infection.

1. Set an Administrator Password

The first, and probably most important, precaution you can take is to set an Administrator password on your machine if you are running any of the most current Windows systems (e.g., XP, ME, 2000). If you don't, you're making your computer very vulnerable indeed, for there are multiple worms and viruses that can exploit this single vulnerability.

Running a Windows system without having set an Administrator password is comparable to leaving the door to your house unlocked: anyone can just come in and rummage through your things, and potentially could even move right in. When the Administrator password has not been set, someone else can log in to your computer, use it, copy files to it, and even use your computer to launch attacks against other computers. Setting the Administrator password is like locking your door against these intruders.

To set your administrator password:

- Press "Ctrl+Alt+Delete" on your keyboard.
- Click on the "Change Password" button.
- Type "Administrator" in the "User Name" box.
- Select "this computer" in the "Log on to:" drop-down box.
- In the "New password:" box, type a secure password.

If you do not see a box appear with this option when you press "Ctrl+Alt+Delete", then you can access this same section by doing the following:

- Go to the "Start" menu.
- Click on the "Control Panel" button.
- Double click on the "User Accounts" button.
- Click on the account name for which you want to set the password.
- Click on the "Change my password" selection.
- In the "Type a new password" box, type in a secure password.
- Retype the password in the "Type the new password again to confirm" box.
- Click on the "Change Password" button.

2. Apply All Critical Patches from Microsoft

Another important step in securing your Windows machine is to keep up-to-date with any critical patches that Microsoft releases. Microsoft and other manufacturers release these updates, which run on your computer to repair newly found vulnerabilities in their software. In the past few months, Microsoft has released a number of critical patches for some serious vulnerabilities.

We strongly recommend that you configure Microsoft's "Windows Update" program to automatically check for new patches. To do this:

- Connect your computer to the Internet. Go to the lower left-hand corner of your screen and click on "Start", to open the Start menu.
- Choose "Windows Update" from this menu. If "Windows Update" is not included in this list, click on "All Programs"; you should now see "Windows Update".
- Next, click on "Windows Update", which will open a new window. On the right-hand side of the new window, click on the link that reads, "Scan for updates".
- When the scan is complete (it will take a few seconds), a list will appear on the left-hand side of your screen. Click on the link for "Critical Updates and Service Packs". This will show you a list of all the patches you need to install; we recommend that you do not run more than five at a time.
- If you are installing patches on a laptop computer, be certain that your machine has plenty of battery power, or is plugged in before you begin.
- Although it may take some time to install the patches, it is very important to use them all.
- Once the installation is complete, you will be asked to restart your computer. After doing so, go back to the beginning and start the process over again. Keep doing this until no critical updates appear when you select "Scan for updates".

Once your computer is completely up-to-date with all of the Critical Updates, make a point of checking Windows Update daily, or you can set Windows Update to automatically download and install any newly released patches. See the following Microsoft article for a complete step-by-step guide on how to do this for your specific operating system: <http://www.microsoft.com/security/protect/>.

3. Install and Run Anti-virus Software

Another key layer of protection for your machine is anti-virus software. This type of software runs on your machine, constantly monitoring for any virus or worm-type activity. If this type of activity is detected, you will receive a warning from the program with a request to either clean or delete the infected files.

Through a site-license acquired by ITS, NYU provides Symantec Anti-Virus software to qualified members of the University community at no cost to the individual. You can download this package from the Software channel in the Files tab of NYUHome,

or from the latest NYU-NET CD, available at the ITS Client Services Center, 10 Astor Place, 4th floor (see <http://www.nyu.edu/its/csc.html> for hours).

Once you have installed anti-virus software, it is vitally important that you keep your virus definitions up-to-date. Anti-virus programs use these definitions to recognize new viruses and worms—without the definitions, your software can't catch and repair them. By the time that you have installed any type of anti-virus software on your machine it is most likely already out of date, so be sure to check for updates immediately after installing the software.

After that, you should check for new definitions daily; you can configure most anti-virus programs to check for and download these updates automatically. Remember: your anti-virus software is only as useful as it is up-to-date.

4. Keep in the Know!

ITS will post virus notifications to the Security channel within NYUHome. Keep an eye on this channel for up-to-date security news. Also, check for virus alerts and instructions on how to download specific virus cleaning tools at the ITS Security website: <http://www.nyu.edu/its/security/virus.html>.

Additional Information

These are the four simple steps that every person who uses a Windows computer should take to help secure their machine. For more advanced protection, you may want to look into the many configuration guides and tools offered by Microsoft and the Center for Internet Security. To see a list of all of Microsoft's Security Tools and Checklists, click on the link for Security at <http://www.microsoft.com/technet/>. The Center for Internet Security can be found at <http://www.cisecurity.org>.

If you have any questions, contact the ITS Client Services Center at 1-212-998-3333 or its.clientservices@nyu.edu. Thank you for helping to keep NYU's network safe!

Author Biography

Tracey Losco is a Network Security Analyst in ITS Network Services. She can be reached at tracey.losco@nyu.edu.

Page last reviewed: November 4, 2003. All content © New York University.
Questions or comments about this site? Send e-mail to: its.connect@nyu.edu.