


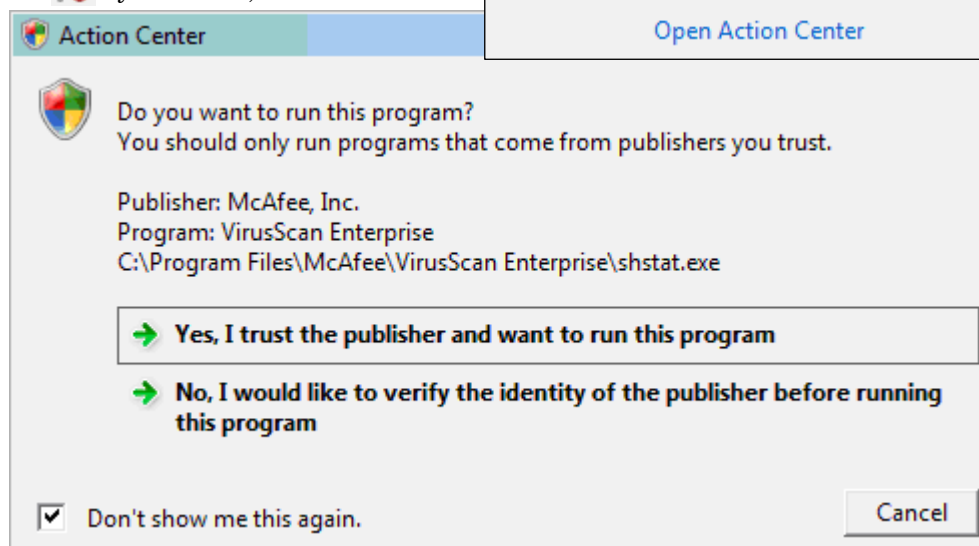
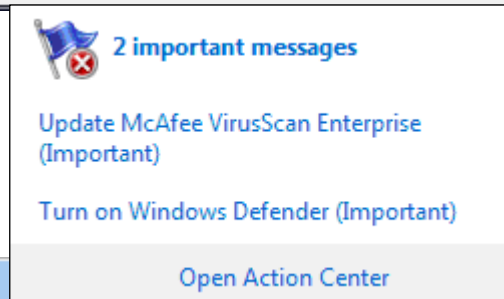
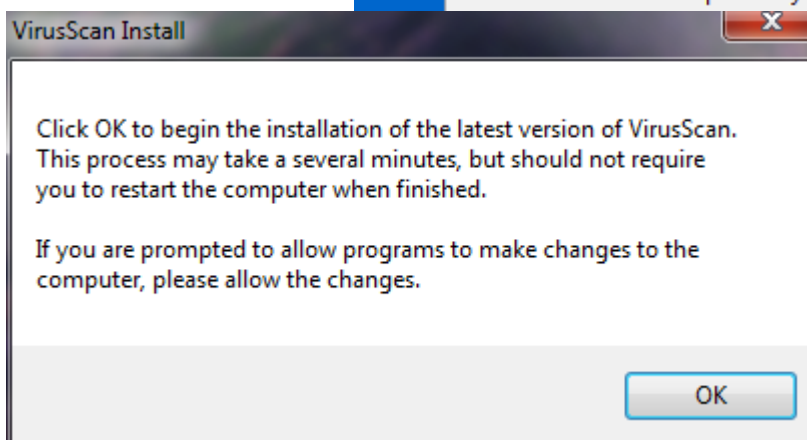
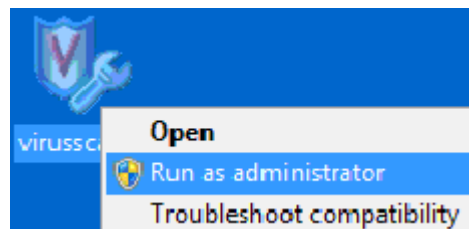
Computer Viruses: McAfee VirusScan 8.7 (Windows XP/Vista/7)

St. Norbert College's license for the McAfee VirusScan anti-virus program permits SNC students, faculty, and staff to install and use the program free of charge on their personal/home computers.

Important: Do not install McAfee VirusScan on a computer running any other anti-virus software, as this can cause serious computer problems. All other anti-virus software **must** be uninstalled first.

Installing McAfee VirusScan 8.7 on Windows 7

1. To download McAfee VirusScan, go to our downloads page at <http://www.snc.edu/techsupport> and click on Download McAfee VirusScan 8.7i. Save the file on your computer, taking note of where it is being saved (the Desktop is the easiest place). When the download is complete, close all open programs.
2. Right-click on the file you just downloaded and choose Run as administrator (shown at right). Do not just double-click on the file; if you do, the installation will fail.
3. When Windows asks "Do you want to allow the following program from an unknown publisher to make changes to this computer?," click Yes (not shown).
4. When prompted to begin the installation (shown at right), click OK.
5. Wait while the installation finishes. It may take quite a while, and at times it may appear to be stuck or frozen and the "Time remaining" indicator may increase or decrease and display inaccurate estimates. As part of the installation, old SNC versions of McAfee VirusScan will be removed. During the installation, you may see other warnings/prompts from Windows Defender or other security programs. Allow all changes.
6. When it says "McAfee VirusScan installation is complete," click OK.
7. At the end of the installation, you may see a notification saying "McAfee VirusScan Enterprise is out of date. Click to update." Click on the Action Center icon  by the clock, then click on "Update McAfee VirusScan Enterprise (Important)" (shown at right).
8. When it asks if you want to run the program, check the "Don't show me this again" box at the bottom, then click on "Yes, I trust the publisher and want to run this program" (shown at right).
9. The initial update may take a while to install. Wait until it finishes.



Updating McAfee VirusScan 8.7

New viruses are being created all the time, and the only way to protect against them is to keep your anti-virus software up to date. The College's version of McAfee VirusScan 8.7i is configured to automatically check for and download updates regularly. To download the latest updates manually at any time, just right-click on the McAfee "V" shield icon by the clock and choose Update Now.

Using McAfee VirusScan 8.7

If your computer is infected with a virus, do not use it until the virus has been successfully eliminated. While scanning your computer for viruses, disconnect it from the network/Internet so that it does not spread viruses.

In Windows XP, you first need to turn off System Restore, because it can keep viruses from being properly removed. Note that turning off System Restore will delete all available restore points.

1. Right-click on My Computer and choose Properties (or go to Start ► [Settings] ► Control Panel ► [Performance and Maintenance] ► System).
2. On the System Restore tab, check the box next to "Turn off System Restore" and click OK.

Then, to begin the virus scan:

1. Go to the Start ► Programs ► McAfee ► On-Demand Scan.
2. By default it will scan all local drives. If you wish to scan only a specific drive, file, or folder, highlight All local drives, click the Edit button, change the drop-down list to "Drive or folder," click the Browse button, locate and highlight the desired drive, file, or folder, and click OK.
3. The "Include subfolders" and "Scan boot sectors" boxes should be checked.
4. Click on the Start button. The VirusScan program will scan the drive(s), folder(s), or file(s) you chose and report if it finds any viruses. If you are scanning all fixed drives this may take quite a while.
5. If VirusScan finds viruses, it will try first to clean them, then if it cannot clean them, it will try to delete them. If it reports that it cannot clean or delete an infected file, have it move the file to the quarantine folder, then proceed.
6. When the scan is complete, close all programs and restart your computer.
7. If VirusScan reported that it could not clean or delete an infected file, run the full scan of all fixed drives again to make sure it finds nothing. (It often reports that it couldn't remove something even though it actually already has removed it.) If it still reports that it cannot clean or delete a file, write down the name of the virus(es) and infected file(s), finish the scan, then contact the Help Desk for further instructions.
8. If you have Windows XP and turned System Restore off, turn it back on (Start ► Control Panel ► [Performance and Maintenance] ► System, uncheck the box next to "Turn off System Restore," then click OK).

Protecting yourself from viruses

- **NEVER** open, view, or execute any file you receive as an e-mail attachment until you have confirmed that it is virus-free. Be suspicious of **all** e-mail attachments, no matter what type of file it is or who it's from. *Even if you know and trust the person who sent the attachment*, it may still contain a virus. When you receive an attachment, first save the file *without* opening it, then use your anti-virus software to scan the file before opening it.
- Keep your anti-virus software and virus definitions up to date. Anti-virus software is useless if you don't keep it up-to-date. On all campus-owned PC computers connected to the network, IT automatically updates these virus definitions as they become available. At home, you should update your virus definitions at least monthly (weekly is best). Although there are many Macintosh viruses, Mac users on and off campus should update their virus definitions monthly.
- Keep all of your software – e-mail program, web browser, Microsoft Office, etc. – up-to-date by installing all updates and patches. On campus-owned computers, this is not necessary for standard network software, as IT supplies these updates automatically. On other computers, run the Windows Update (Start ► Windows Update) to patch the operating system. Routinely check the web sites of all of your software programs for the manufacturer's updates/patches.

- For maximum protection, configure your anti-virus program to automatically scan all e-mail, Internet downloads, disks that are accessed, and files/documents that are opened.
- Keep backup copies of all computer files you do not want to lose. That way, if your computer becomes infected, you will still have copies of your files that are not infected. The copies should be stored in separate locations, for example, on your hard drive and on a CD.

What are computer viruses?

Computer viruses are computer programs, created by people, which take control of your computer without your knowledge. They can affect your computer files and disks, and often replicate themselves. Computer viruses can be destructive or non-destructive. Destructive viruses perform harmful operations such as deleting files or introducing errors into documents. These types of viruses often make files, and even entire disks, unusable. Non-destructive viruses may do things such as display a message or picture on your screen.

How are computer viruses transmitted?

Viruses can hide almost anywhere: floppy disks, flash drives, hard drives, networks, CDs/DVDs, documents, programs, games, and e-mail attachments. If a removable disk/drive becomes infected, any computer into which that disk/drive is inserted may also become infected. If an infected file is opened, the drive on which it is run will be infected. If an infected e-mail attachment is opened, the computer on which it is opened will be infected, and it may attach itself to every e-mail message sent from the infected computer. Once viruses infect one computer or disk, they can spread rapidly to many computers.

How do you know if your computer has a virus?

Unusual activity on your computer can be a sign of a virus. Watch out for the following things. (Note: These things can be caused by problems other than virus infection.)

- Pop-up windows (this may also be a sign of spyware or adware)
- Warning messages from your computer or anti-virus software
- Unusual error messages
- Programs or files that mysteriously disappear or won't open
- Programs that take abnormally long to load

Viruses and hoaxes

There are many myths and hoaxes about computer viruses that circulate via e-mail. Be aware that most of these virus alerts are hoaxes. There are people who write false alerts, and many more people who pass on those alerts to everyone they know without checking the facts. If you receive a virus warning message from anyone other than the St. Norbert College Tech. Support or IT departments, do **not** forward it to anyone without first verifying it with an authoritative source. If you wish, you may forward it to helpdesk@snc.edu for verification.

Helpful web sites

- Network Associates (makers of McAfee VirusScan software): <http://home.mcafee.com/VirusInfo>
- Symantec (makers of Norton AntiVirus): http://www.symantec.com/norton/security_response/threatexplorer
- Hoaxbusters: <http://www.hoaxbusters.org>
- Computer Virus Myths: <http://www.vmyths.com>

Assistance and questions

If you have any questions or need more information, contact the Help Desk at (920) 403-HELP (4357) or helpdesk@snc.edu. The Help Desk is for St. Norbert College students and employees only.