

# Antivirus Software

## The Trinity of Antivirus Protection

### 1. Use Antivirus Software Properly

Syracuse University requires that antivirus software be installed and running on all computers connected to the University's network. [A list of recommended AV products can be found at this link.](#)

Once installed, antivirus software must be regularly updated so that it can detect and eliminate the latest viruses that attack your computer. ITS recommends that you either manually check for updates for your antivirus software weekly, or configure your computer to automatically check for updates on a daily basis. In addition, you should completely scan your system for viruses at least once a week.

### 2. Update Your Machine's Operating System

Computer software often has security holes that can be found and exploited by viruses, worms, and Trojans. When security holes are discovered, software companies post patches and fixes on their Web sites; however, it is up to computer owners to apply the patches to their machines.

To ensure that your computer is updated with the latest security patches and fixes, visit the company Web sites on a regular basis. If you are running a Microsoft Windows operating system (XP, Vista, etc) you can configure your computer to automatically check for updates to the software, or visit <http://www.microsoft.com/security/protect/> every week to check for the latest updates.

Information about obtaining security updates for Macintosh operating systems is available on the Web at <http://www.info.apple.com/usen/security/index.html>

### 3. Avoid Strange Email Attachments

Never open e-mail attachments unless you confirm the source and are expecting the attachment. Do not open attachments with file extensions such as ".VBS", ".EXE", or any extension with which you are not familiar.

Beware of "spoofed" e-mail addresses in the "from" message box. The address may contain a name you recognize, but the person may not have sent the message. Hijacking e-mail addresses is a technique used by spammers and virus programs.

When in doubt, delete all suspicious e-mail messages. Do not reply to the sender. The act of responding to suspicious e-mail will validate your e-mail address and may result in future e-mail harassment. Bottomline: If something looks unusual in an e-mail, **DELETE IT!**

## Information for ResNet Subscribers

### *Student Antivirus:*

Syracuse University requires all computers connected to the University's wired or wireless networks be protected by a current version of antivirus software. Students should choose from the University's [list of recommended antivirus software](#).

*Questions:* Contact ITS at [help@syr.edu](mailto:help@syr.edu) or 443-2677.

**IMPORTANT NOTES:** Many new computers come with trial or demonstration versions of antivirus software. These trial versions do not meet SU requirements. Students need to verify that the antivirus software installed on their computer is a fully licensed version.

## Information for Faculty, Staff & off campus students

Antivirus Information for Faculty, Staff and Off-Campus Students Syracuse University requires that antivirus software with auto updates be installed and running on all computers connected to the University's network. A list of recommended AV products can be found [at this link](#).

*Additional Information:* [McAfee Security](#): This Web site contains information on the latest viruses and how to identify hoaxes. The site also provides help for removing viruses from computers.