



@ Saint Mary's College

<http://www.saintmarys.edu/resnet>

Protect Your Computer from Viruses and Malware!

What are viruses, trojans, worms, and malware?

Viruses are programs designed to spread from one computer to another and to interfere with your computer use. Viruses can infect your computer simply by you opening e-mail attachments or visiting infectious websites via "drive-by downloads." Viruses can slow down your computer, prevent Internet access, delete data on your computer, and use your e-mail program to spread themselves and your personal data to anyone you know (and even people you don't).

Trojans are frequently disguised as freeware you would otherwise pay for, including peer-to-peer file sharing of music, videos, and pirated software. Trojans do not self-replicate. Trojans can give others complete access to your computer and report every keystroke you make. They can disable your virus protection and firewall software, and pretend to be anti-virus software when they are not.

Worms can infect your computer simply by having the computer connected to the Internet without current software patches installed. Worms are self-spreading.

Malware refers to any malicious software on a computer.

How can I protect my computer?

- Always have up-to-date virus protection software installed on your computer. Saint Mary's provides Bitdefender security software for free to all students for their College-owned and personally-owned Mac OS X/MacOS and Windows computers.
- If a message (e-mail, IM, text) isn't personalized, don't click on the links or open the attachments. You should never open an attachment you are not expecting.
- Don't click on any link if you are not 100% certain where it will go. Stick with reputable websites for your information. Not every link found with Google is a safe one.
- If a free copy of software/music/video sounds too good to be true, it probably is. It could be bait for a drive-by (hidden in the background) download of malware.
- Make sure you are always using the latest version of Adobe Flash. It should be downloaded directly from www.adobe.com and NOT from any other website that prompts you to install it.

- If you believe your computer may have malware currently being installed (for example, you see a suspicious pop-up about anti-virus or anti-malware software), push the power button on your computer and hold the button in until the machine turns off. Do not click on the cancel or X buttons in the windows.
- If you have installed a Windows operating system on an Apple computer, that computer is just as vulnerable to malware as any other computer running Windows. Make sure that you take the same precautions as other Windows users to protect your computer – keeping your version of Windows up-to-date with Windows Update and installing and keeping your Windows virus protection software up-to-date (in addition to your Mac OS X virus protection software).

What happens if my computer becomes infected?

- If your computer is infected with malware, you are responsible for cleaning the unwanted software off your computer. Instructions for removing many current threats are available on the ResNet FAQ at <http://www.saintmarys.edu/resnet/resnetfaq>
- The ResNet Office can provide assistance with malware removal, but the process may take several hours. You must be present with your computer in the ResNet Office the entire time your computer is being worked on.
- Saint Mary's College and Information Technology are not responsible for any loss of data or other damage caused by malware. You are responsible for backing up your personal files on a regular basis. Your personal network drive is backed up automatically every night by Information Technology, and access to Google's G Suite for Education includes Google Drive for quotaless cloud storage of your files.
- If your computer is infected with malware that is self-spreading (via e-mail or over the network in some fashion) or your computer is suspected of having malware because it is displaying symptoms of infection over the network, Information Technology will block Internet access from your computer until the infection has been removed and the ResNet Office has witnessed a scan for malware on your computer indicating the computer is clean.

How Can I Protect My Computer Against Malware?

In a networked environment such as Saint Mary's College (including ResNet), the ease with which malware can spread from computer to computer is greatly multiplied, as is its potential for damage. Instead of affecting just your machine, malware could spread to hundreds of computers all over campus, and could even bring down our campus network. Recognizing this threat, the College has decided to provide virus protection software *free of cost* to all students, faculty, and staff for their personal computers. This software can be downloaded from the campus network and installed on your computer. **Any student who connects her computer to the Saint Mary's network via ResNet must install virus protection software and keep it up to date.** Failure to have current virus protection software on your computer may result in the loss of ResNet access privileges. Bitdefender security software is available for both Mac and Windows computers. Instructions for installing virus protection software on your personal Mac or Windows computer connected to ResNet can be found at:

<http://www.saintmarys.edu/virus>