



@ Saint Mary's College

www.saintmarys.edu/resnet

Protect Your Computer from Malware and Security Threats!

What are these threats, and are they serious?

Malware refers to any malicious software on a computer. Security threats could include malware or any other type of unauthorized access to your computer. If your computer is compromised by malware or another threat, you could encounter slow performance, limited to no Internet access, the deletion of data from your computer, files and personal information distributed over the Internet from your computer without your knowledge, record every keystroke you make (including passwords and credit card information), and give individuals complete access to your computer without your knowledge or permission.

How can I protect my computer?

- Always have up-to-date security software (such as virus protection) installed on your computer. Saint Mary's provides Bitdefender security software for free to all students for their personally-owned macOS and Windows computers.
- If a message (e-mail, chat, 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.
- 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 security software up-to-date (in addition to keeping your version of macOS up-to-date and keeping your macOS security software up-to-date).

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 to protect your personal information and to prevent the malware from affecting others. Instructions for removing many current threats are available on the ResNet FAQ at <http://www.saintmarys.edu/resnet/resnetfaq>
- The ResNet Office provides 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 Google's Workspace 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, 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 provides Bitdefender security software *free of cost* to all students, faculty, and staff for their personally-owned computers. Any student who connects her computer to the Saint Mary's network must install security protection software and keep it up to date. Failure to have current security protection software on your computer may result in the loss of BelleNet access privileges. Bitdefender security software is available for both Mac and Windows computers. Instructions for installing security protection software on your personal Mac or Windows computer connected to ResNet can be found at:

www.saintmarys.edu/virus