Marshall University
SYMANTEC ANTIVIRUS

MARSHALL UNIVERSITY CAMPUS LICENSE FOR SYMANTEC PRODUCTS

ALLOWS OUR STUDENTS, FACULTY AND STAFF TO INSTALL THE ENDPOINT PROTECTION (ANTI-VIRUS/ANTI-MALWARE) PRODUCT ON THEIR PERSONALLY-OWNED COMPUTERS. PLEASE USE THE FOLLOWING INSTRUCTIONS TO DOWNLOAD AND INSTALL SYMANTEC ANTIVIRUS PROTECTION.

» HOW TO ACCESS AND INSTALL SYMANTEC

1. Go to www.marshall.edu/antivirus

2. Select the Unmanaged version if installing on an off-campus or personal computer

3. Select the Managed version if installing on a University owned computer.

4. Select the appropriate download for your system. *If you are not sure if you have a 32 or 64 bit based Windows computer, simply right click the start/Windows button and click "System". This will display what version you are currently running.

5. You will be prompted for your MUNet login credentials.

6. The software will begin downloading, once finished, open the folder.

7. Double click on the Setup File to begin installation. *In some cases, you might have to extract the folder.

8. Follow the instructions to complete the installation.

Questions?
We're here to help!

Stop by the Information Center on the first floor of Drink Library.

Email: itservicedesk@marshall.edu Phone: (304) 696-3200
Website: www.marshall.edu/it

AVOIDING AND ADDRESSING MALWARE INFECTIONS

» HOW TO AVOID A MALWARE INFECTION:

- ❑ **Backup your data often.** If your computer becomes infected or damaged, you will still have a backup which you can use to restore your data to another device.
- ❑ **Install antivirus protection on your computer.**
  - If you are a student, faculty or staff member, download Symantec Endpoint Protection free at www.marshall.edu/antivirus.
  - Configure your antivirus program to scan your computer daily.
  - Keep virus signature definitions up-to-date. Most antivirus programs update virus definitions automatically or will notify you if a problem arises.
- ❑ **Make sure your operating system is set to update automatically.**
  - Windows: Settings > Update & Security > Windows Update > Install Updates Automatically
  - Mac: System Preferences > App Store > "Automatically check for updates" and "Download newly available updates in the background"
- ❑ **Keep up with software updates.** Some apps update automatically, but many will ask for your permission to update. While these can be an annoyance, do not put these updates off – they can prevent cyber-criminals from infecting your computer.
- ❑ **Be cautious before opening email attachments and clicking on links within emails, even from people you know.** Cyber-criminals can falsify the sender's address or your friend or family member's account could be compromised and used by a cyber-criminal to send malicious emails.
- ❑ **Be careful downloading files and programs from the internet.** Many programs appear to be safe, but will trick you into installing adware or spyware without your knowledge. When in doubt, contact the IT Service Desk and ask them if the program or file is safe.

» WHAT TO DO IF YOU THINK YOUR COMPUTER IS INFECTED:

- ❑ **Do not continue using your computer** for further work, add files that contain personal information, or use the web to login to financial, personal, or work accounts.
- ❑ **Record all error messages and details of the issues you experience.**
- ❑ **If you have antivirus software, make sure the virus definitions were updated within the last 24 hours.**
  - If not, manually update the definitions. Your antivirus should have a button which allows you to do this. If you are using Symantec Endpoint Protection, open the program and click "LiveUpdate…"
- ❑ **Make sure you have applied all of the latest operating system patches.**
  - Windows: Settings > Update & Security > Check for Updates
  - Mac: App Store > Updates
- ❑ **Remove your computer from the network** – either unplug the Ethernet cable or disable any wireless connections.
- ❑ **Use your antivirus program to run a full scan on your computer.**
- ❑ **Contact IT Support** – either your departmental IT support technician or the MU IT Service Desk. They can perform the steps above for you if you prefer to contact them first. They will also perform additional steps to make sure your computer is clean and free of malware.

Questions? We're here to help!