Antivirus Software and Malware Protection

Overview & Key Terminology

The terms "virus" and "malware" are often used interchangeably. However, they are technically different, so the question of malware vs. viruses is an important one.

Malware is a catch-all term for any type of malicious software, regardless of how it works, its intent, or how it's distributed. A virus is a specific type of malware that self-replicates by inserting its code into other programs.Viruses spread by attaching themselves to legitimate files and programs, and are distributed through infected websites, flash drives, and emails. A victim activates a virus by opening the infected application or file. Once activated, a virus may delete or encrypt files, modify applications, or disable system functions. Ransomware is a type of malware that demands a ransom in order to be removed. For more info about ransomware, visit https://answers.syr.edu/x/aSCfAg

Adware is a type of malware that is more annoying that it is detrimental to the inner workings of your machine. Most commonly seen as a google search that doesn't allow you to actually see your results or a barrage of pop-ups. Adware pushes unwanted advertisements at users.

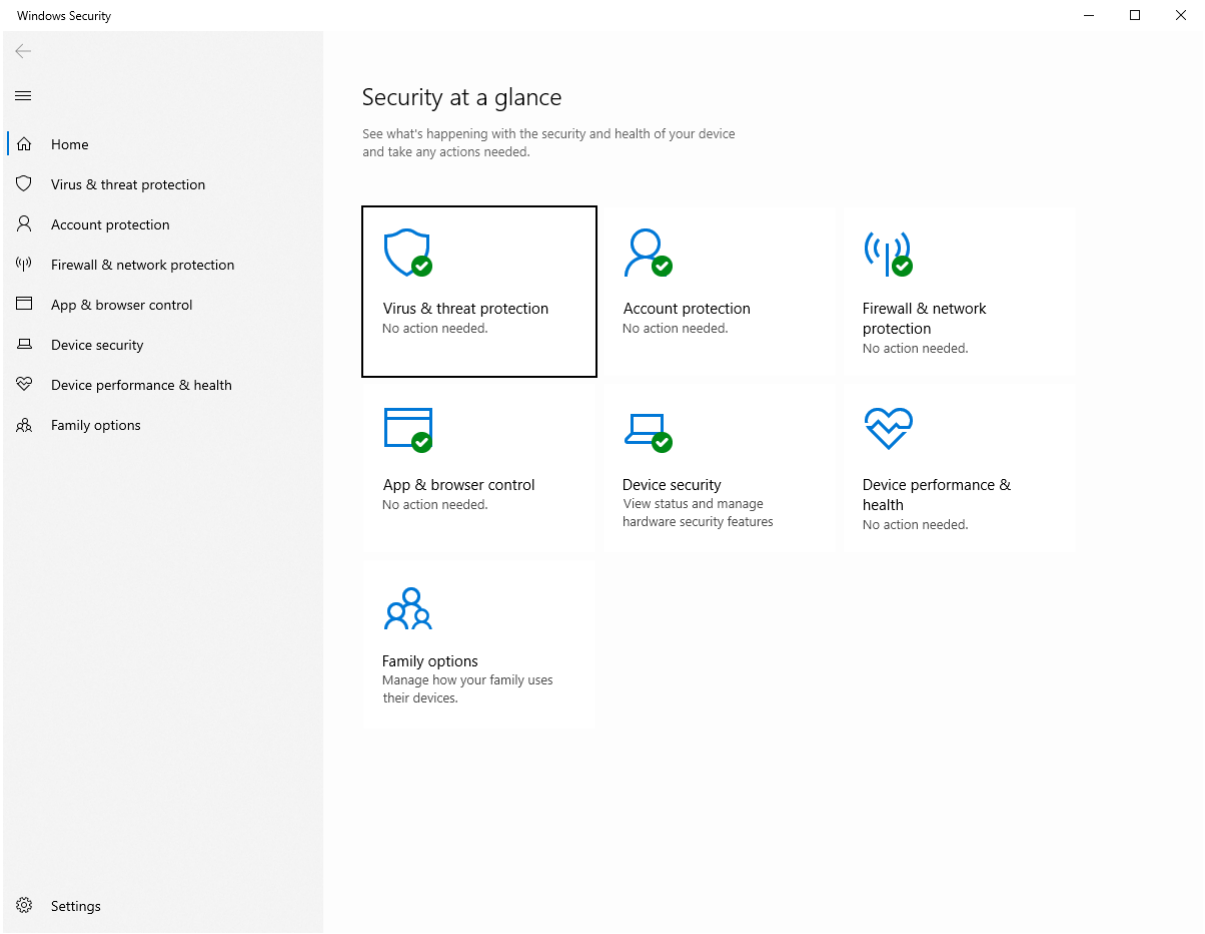
Spyware secretly collects information about the user. Spyware may record the websites the user visits, information about the user's computer system and vulnerabilities for a future attack, or the user's keystrokes. Spyware that records keystrokes is called a keylogger. Keyloggers steal credit card numbers, passwords, account numbers, and other sensitive data simply by logging what the user types.

Trojans pretend to be legitimate software, but run malicious code not immediately visible to the user. To avoid trojans, only download applications from verified vendors and trusted websites.

Depending on the type of operating system you have, you should have some default antivirus protection but may need to supplement with additional malware protection.

Windows 10 Recommendations

- For Windows 10 computers, we recommend using the built-in Windows Security. Security experts consider it to be a powerful defense against virus and other threats. 3rd party antivirus software is generally not needed on Windows 10 machines.
- Windows Security is enabled by default on Windows 10 machines, but if you want to make sure it is enabled, simply type Windows Security in the start menu, click on Windows Security, and make sure there is a green checkmark next to all settings as shown below.
- Always allow Windows updates to run to ensure Windows Security is up to date.



macOS Recommendations

- Mac computers build on the unique capabilities of Apple hardware and have a system security is designed to maximize the security of the operating systems on Apple devices without compromising usability. System security encompasses the boot-up process, software updates, and the ongoing operation of the OS.
- Technologies like XD (execute disable), ASLR (address space layout randomization), and SIP (system integrity protection) make it difficult for malware to do harm, and they ensure that processes with root permission cannot change critical system files.
- As long as your Mac is up to date with the latest operating system, as of June 2021 that is Version 11.0 Big Sur, then your Mac has protection from viruses that can do harm.
- As a supplemental precaution, we recommend downloading an AdWare/Spyware remover program called MalwareBytes. Any computer that can connect to the internet can get malware but most times it is quickly and easily removed by running an industry standard program like MalwareBytes.

Adblock - Block YouTube ads & help protect yourself from some types of malware

- Advertisements and popup links on websites may claim to provide a free app or service, but many times these links are malicious and result in a malware infection.
- To avoid this risk, and to potentially improve your web-browsing experience by blocking intrusive ads, including YouTube ads, use Mozilla Firefox or Google Chrome as your web browser and install the uBlock Origin ad-blocker addon via one of the links below:
  - Mozilla Firefox installation link: https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/
  - Google Chrome installation link: https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm?hl=en
- While browsing SU websites or any other website you fully trust or may want to support by allowing advertisements, disable uBlock Origin by clicking on it's icon  at the top-right of your browser, then click the "power" icon which will disable it only for the website you are currently visiting.

> Note: uBlock Origin is a free 3rd-party tool not provided by or directly supported by ITS

I am using these security tools and I think I have a virus! What should I do?

- Consider downloading a 3rd party anti-malware program called Malwarebytes. It can catch some infections your PC's built-in security software might have missed.
- You can download Malwarebtyes for Windows or Mac here: https://www.malwarebytes.com/mwb-download/ (Make sure to choose the free version!)
- **If you are not sure how to operate Malwarebytes or think your computer may still have a virus, feel free to bring your machine to the Service Center**! We can assist in scanning your machine, or potentially resetting your machine and backing up your data if needed. A full reset of your computer is often the only way to remove 100% of computer infections.
- Service Center hours, location, and other details can be found here: https://its.syr.edu/its_service_center/

I have three antivirus programs running and now I can't access the internet

- When it comes to antivirus programs, too much is a bad thing. What can begin to happen is the programs start detecting each other as problems and can begin to cause internet connectivity issues and overall slowness on the machine. If you feel this may be happening to your machine, please feel free to call the Help Desk at 315-443-2677.