(http://www.uni.edu/its)

Use Anti-Virus and Anti-Spyware Software

Protecting your Home Computer

Anti-virus and anti-spyware software, more easily defined as anti-malware software, are probably the most important pieces of software any Windows system can have. While Macs, Linux, and other systems are vulnerable to virus and spyware attacks as well, the design of their systems and their lower market share has made them less desirable to malicious software developers.

PLEASE NOTE:

This article is intended for personally-owned machines only. UNI systems should have their anti-virus and anti-spyware software managed by the appropriate support staff.

Why do they want to Attack my System?

The rational behind malware (**MAL**icious soft**WARE**) various greatly, but the number one factor is money. Some of the most widespread malware has been used to send SPAM or to have the machines act as attackers in a distributed, mass-attack on websites or networks. Some malware is designed for identity theft, others for making money off ads or the sale of products. There are some that are just plain malicious for the sake of being malicious. Others may be intended for corporate espionage or international spying. Anti-virus companies are increasingly finding malware that was designed for a specific institution's network structure.

Best Practices for all Anti-Malware Software

The goal of any anti-virus or anti-malware software should be to prevent the software from entering the system in the first place. Secondly, if malware is successful in entering the system, the anti-malware software should help you remove it or at least inform you of an infection so appropriate action may be taken.

For any anti-malware software to be successful, it must be up-to-date and receiving definitions automatically from the distributor. Many home users will find that their anti-malware software has expired and is not receiving updates. If that is the case, a renewal must be purchased, or a new program installed. Good software will update itself automatically. Some free anti-spyware programs will require manual updates.

In general, it really does not matter how you got any piece of malware, the end result is the same, it needs to be removed. Sometimes the only method to clean an infected system is to reformat the computer and reinstall the operating system. In this situation, your data should be restored from backups.

NOTE: You should only run one anti-virus software program at a time. Installing more than one at a time will cause system instability and may make the software ineffective.

Windows Users

Windows machines are nearly guaranteed to be infected with some form of malware without adequate software protection.

Even then, some malware may sneak by the software. There are literally hundreds of anti-virus applications out there, many are available at various retailers. You should make sure the software solution you choose provides adequate protection. Many of these programs may not be used on institutional computers and are only licensed for non-commercial home use. Free anti-malware software for home users running Windows can be found on the free software page [1].

Mac Users

Macs have seen some share of malware, but mostly Mac anti-virus software scans your documents for Windows viruses, so you do not inadvertently pass them on to your Windows-using friends. Many Mac users run without any anti-malware software. This strategy may work, but care should be taken to protect the system with adequate software should the status quo change. Ideally, Macs should be running anti-malware software of some sort, to prevent a devastating outbreak should one be written. Free anti-malware software for home users running Macs can be found on the free software page [1].

Linux Users

Linux machines have seen some malware, but mostly Linux anti-virus software scans your documents for Windows viruses, so you do not inadvertently pass them on to your Windows-using friends. Many Linux users run without any anti-malware software. This strategy may work, but care should be taken to protect the system with adequate software should the status quo change.

ClamAV [2]	Free virus dection program.

Virus, Spyware, Adware, and Malware Defined

The differences between the various types of malicious software has led to numerous terms to classify the various types of malicious programs based on how they infect the system and what they do once the system is infected. Really, you do not want any of these nasty software programs on your computer and its easy to call them all malware (malicious software).

Here basic descriptions of some of the various terms:

Virus [3]	Software designed to copy itself and typically has a detrimental effect on the system or data stored on it. A virus typically has to be loaded onto the computer is some fashion, usually by an infected file.
Spyware [4]	Software designed to track the use of a computer system, especially on the internet, for marking purposes or for identity theft.
Adware [5]	Software that displays ads on the computer. Some adware is not necessarily evil, but offers you free software in exchange for ads. Some adware is exceptionally evil, bombarding the computer with many ads--some pornographic and replacing ads on websites with those the adware author desires to show.

Worm [6]	Simply speaking, a worm is like a virus that is capable of spreading itself over the network autonomously, so a machine can become infected even if it was doing nothing but sitting idle. Worms usually cause more harm to the network and usually do not target the files on the system.
Trojan Horse [7]	A trojan horse is an innocent-looking software program that actually delivers a malicious payload in addition to preforming the advertised function.
Rootkit [8]	Rootkits are virtually undetectable as they replace the core portion of the operating system with their own code. They are usually able to hide themselves from anti-virus/anti-spyware software if they are not caught in the initial infection attempt. Unless a specific removal tool is available for a particular rootkit, the infected system must be wiped clean and reinstalled from scratch to ensure the security of the system. In Unix-based systems, the root user is the ultimate administrator, hence the name rootkit

These malicious programs may install some of the following:

Backdoor [9]	Malicious software or system changes that make it easy for intruders to take control of the system.
Dialers [10]	Less common now that many machines are not connected via a dial-up connections, but they still exist. These programs use the attached modem to call premium-rate telephone numbers owned by the author.
Keyloggers [11]	Malicious software that logs the keystrokes on the computer, sometimes even more detailed logging of the system. Keyloggers are usually looking for passwords or personally identifiable information that may be used for identity theft.
URL Hijackors [12]	Malicious software that redirects users to sites they prefer. For example, a URL injector may redirect www.google.com [13] to its author's search site, so the author can make money.

Of course, some malware attacks include many of the above items or may consist of multiple malware programs combined together.

Links:
[1] http://www.uni.edu/its/software-hardware/players-and-viewers
[2] http://www.clamav.net/download/packages/packages-linux
[3] http://en.wikipedia.org/wiki/Computer_virus
[4] http://en.wikipedia.org/wiki/Spyware
[5] http://en.wikipedia.org/wiki/Adware

[6] http://en.wikipedia.org/wiki/Computer_worm
[7] http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29
[8] http://en.wikipedia.org/wiki/Rootkit
[9] http://en.wikipedia.org/wiki/Backdoor_%28computing%29
[10] http://en.wikipedia.org/wiki/Dialer#Fraudulent_dialers
[11] http://en.wikipedia.org/wiki/Keystroke_logging
[12] http://en.wikipedia.org/wiki/DNS_hijacking
[13] http://www.google.com