

What is Malware and How Can I Protect Myself From It?

1. Malware – Stands for **Malicious Software**

- a. According to Wikipedia, there are twelve identified types of Malware:

Viruses	Worms	Wabbits (really!)	Trojans
Spyware	Backdoors	Exploits	Rootkits
Keyloggers	Dialers	URL Injectors	Adware

- b. Spyware usually designed to spy on you and steal personal information from your computer. Keyloggers fit into this category by monitoring your keystrokes for credit card info, passwords, etc. This info is then usually sent to another computer without your knowledge.
- c. Viruses usually attach themselves to files or programs and cause damage to your operating system, data files, and personal data. Some can completely wipe your hard drive and cause damage to your operating system. These are usually spread through email attachments, but can't be spread without human interaction.
- d. Worms act and can spread similar to a virus, but do not require human interaction. Worms can replicate themselves and travel using network connections, modems, email, etc. An example is a worm that spreads by attaching itself to an email message and emailing itself to everyone in your address book, **WITHOUT YOUR KNOWLEDGE.**
- e. Wabbits are uncommon, and act only your computer, and do not have an automatic mechanism for moving to another system. Wabbits do not infect host programs or documents.
- f. Trojan's usually hide inside other programs and run when the host program is run. Backdoor's are often installed using Trojans, and allow others to get inside your computer to do whatever they want to do. **NO COMPUTER is 100% safe.** Mac PC's can become infected by malware (usually with a rootkit and/or trojan). However the goal of a malware programmer is to infect as many PC's as possible, so most malware is designed for the majority of computer users who use Windows systems.

2. How to protect yourself from Malware threats? **WASH UP!**

- a. **W – WINDOWS UPDATE:** Install important or critical Windows Updates automatically or install Mac OS patches as soon as they are released to keep your operating system secure.
- b. **A – AWARENESS:** Extreme slow-down of your computer; "unknown recipient" messages in your email box for messages you don't remember sending; badly written emails messages requesting you to click on a link to get a "cool program" or authenticate your account (i.e. phony EBay mail); Out of character email messages from friends/family. ("CLICK for info on this great hair product", from your bald dad!)
- c. **S – SAFETY:** Do not open unexpected attachments, "Notify First!" Do not click on links that are from unknown or un-trusted sources, especially social network sites such as FaceBook, My Space, Twitter, etc.
- d. **H – HELP:** When in doubt, call an expert. (Like me!) Just don't use an email message!
- e. **U – UPDATE:** Renew your subscription to be sure your virus signatures are kept up to date.
- f. **P – PROTECTION:** Run good anti-virus/anti-malware software and a firewall. Recommendation: NIS 2009 (commercial), AVAST (free), BitDefender (Free or Commercial). Perform a full scan regularly, at least once a week. Also, run a good firewall. Windows XP and Vista have a built in firewall, but commercial programs are often better. A combination hardware and software firewall is best.