# How to avoid Malware

Malware is a term that describes a relatively broad category of malicious software including viruses, worms, trojan horses, rootkits, spyware and adware.

**Network Administration - Malware is a term that describes a relatively broad category of malicious software including viruses, worms, trojan horses, rootkits, spyware and adware** . The impact of malware extends from simple to frustrating feelings to computer crashes and even higher identity theft. Malware is actually easier to avoid than to remove it. Avoiding malware is usually a two-part strategy.

**Prevent malware through online behavior online**

The biggest factor in preventing the infection of malware on your computer is in you. You do not need to have knowledge as an expert or need special training, just be cautious about downloading and installing everything you don't understand or don't trust from the following sources:

**From a website** : If you are unsure, leave the site and research the software you are receiving. If all OK, you can go back to the site and install it. If it is unstable, you will avoid the malware trouble.

**From email** : Do not trust anything related to spam e-mail. Note when receiving emails from people you know especially links or attachments. If you suspect what you are asked to view or install, do not follow that

instigation.

**From the physical environment** : Friends, family and colleagues may accidentally give you a CD or a USB containing the infected file. Do not blindly accept these files; Please scan them with security software. If you are still unsure, do not accept these files.

**From the** pop-up **window** : Some pop-ups often invite you to download the software or perform a free system scan. Usually pop-ups will use tips to make you believe you need what they are offering to get safety. Please close the pop-ups without clicking on anything inside it (including the X in the corner of the window). Close the window via Windows Task Manager (press **Ctrl-Alt-Delete** ).

**From another piece of software** : Some programs often try to install malware as part of their installation process. When installing the software, really pay attention to the message boxes before clicking **Next** , **OK** or **I Agree** . If you are unsure, cancel the installation, check the program and run the installation again if you find it completely safe.

**From illegal file sharing services** : You will have to be yourself in this area. There is little quality control in the illegal software world and so it is very likely that attacks will be made through a piece of malware that comes after a good movie, an interesting album or a program. somehow you download it.

**Remove Malware with appropriate software**

No matter how careful you are, you will probably be infected one day. That's because malware is designed to sneak into your computer in so many ways that you can't predict. Therefore, enlist the help of the following software:

**Upgrade operating system** : Use Windows Update. Take advantage of this ability to automatically notify you of updates or even better settings that automatically download and install updates.

**Upgrade your browser:** No matter what **browser** you use, keeping your browser up to date will prevent infection. Use the browser pop-up lock function, download screen and automatic upgrade features.

**Antivirus software** : You must run antivirus software to be safe. However, it is necessary to update it continuously, turn on the software and schedule the scan action at least once a month. (Note not running two antivirus software at the same time because they can conflict with each other).

**Anti-malware:** Also known as anti-spyware, many antivirus applications also contain anti-malware components. If your program does not have this function, install and use a standalone anti-malware program that does not conflict with the antivirus program you are running. Then update it on a regular basis.

**Firewall:** If you do not use a third-party firewall, use Windows Firewall. (Do not run two software at the same time because it can conflict with each other).

**Spam filtering** : If your email program does not filter spam well in the inbox, consider another dedicated spam filtering software. If your security software is a complete security suite, then you need to enable spam filtering available within it.