

Stop From Getting Bite by Malware

By
Scott Sekinger

4/9/12

There are many software programs out on the internet that could hurt your computer and maybe even you. I am talking about Malware. Malware consist of Viruses, Spyware, and other dangerous software. This software could steal your private information, slow down your PC turning it into a weapon to hurt others. This article is not to scare you, but to help you stop yourself from getting bit.

How To Prevent Yourself From Being Bite

You are your best defense. The tips below will help you.

1. Always update Windows, Anti virus software and other software that you use when updates are released. If you do not have an Anti virus program check out <http://www.av-comparatives.org>.. They do a comparison on the different Anti Virus software, and report which is the best. I suggest that you go with Microsoft Security Essential, if you can not afford one. It is not as good as your paid ones, but it the best free one out there. You can get it at http://www.microsoft.com/Security_Essentials/ .
2. Do not click on links in emails that you not expecting. These links could take you to sites that could install Malware on your PC.
3. Do not download software, music, etc from illegal file sharing sites.
4. Think before you install software you just find on the internet. When you find a piece of software you like do some research on it before you use it. The sites below are good sites to do research:
 - a) Cnet's Download.com at <http://www.Download.com/>
 - b) PC Magazine at <http://www.pcmag.com/>
 - c) Tiptenreviews at <http://www.tiptenreviews.com/>
 - d) Tucows at <http://www.tucows.com/>
 - e) Zdnet at <http://review.zdnet.com/filter/software?categoryId=3513>

What To Do When You Think You Were Bite

If you think you are infected by some form of Malware you can do the following to see if you are infected.

1. Change any passwords for personal information as soon as possible, such as banking sites from another PC.
2. Turn off System Restore.
3. Do a Disk Cleanup if you can. This will cut down on the amount of time a scan takes, and get rid of some files that might be infected.
4. Run a full scan with the Windows Malicious Software Removal Tool To do this:
 - a) Click on the <Windows Key> and <R> together, type MRT, press enter and follow the wizard.
 - b) Run a full scan with your Anti-Virus software.
 - c) Run a full scan with an online virus checker. All major Anti virus software companies have one on their website. I suggest using at two online scanners. Some of these online scanners consist of
 - a) Trend Micro's Housecall , which is at <http://housecall.trendmicro.com/>.

- b) Kaspersky's Online Scanner, which is at <http://www.kaspersky.com/scanforvirus>.
- c) Norton Security Scan, which is at <http://security.symantec.com/sscv6/WelcomePage.asp>.
- d) Eset's free online scanner, which is at <http://www.eset.com/onlinescan/>.
- e) Bitdefender's Online Scanner, which is at <http://www.bitdefender.com/scanner/online/free.html>.

If you get a clean bill of health from at least one online scanner, your Anti virus / Antispyware program, Microsoft's Windows Malicious Software Removal Tool then you are probably safe. If your PC still acts very strange then I suggest that you backup your data, and re due your PC. This needs to be done from a good known source, like you System Recovery Disc.