



## “Help, I’m Under Attack!” *by Richard Tausch*

### “How to Win the Battle against Malware”

**Malware**, according to Wikipedia, is short for *malicious software*, software designed to infiltrate a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

So here’s the scoop.....you know something is wrong with your computer since you clicked yes to some pop-up that said you have viruses, or you went to the wrong website by accident and when you closed the page, you noticed an odd message and since then, when you have tried to go to a number of websites, you get redirected to a page that is not the one you wanted, or you get a warning message, or a number of other anomalies seem to be taking place.

In short, the problem is either quite obvious or subtle but you know something is wrong.

**IMPORTANT: Please don’t click on the links at the bottom of this article that contain free Malware removal software yet** because you will need to approach Malware removal programs based on certain conditions as defined below.

If you have Malware, how you approach this is based on either.....

- A) Your system is incapacitated and you literally cannot do anything**
- B) Your system is simply behaving oddly and you can’t put your finger on it**

In the case of A), the Malware may actually cause one of the following that results in:

- 1) Preventing you from going to Malware removal sites

- 2) Preventing you from downloading and installing the Malware removal software
- 3) Presenting an error when you install or run the removal software
- 4) The removal software not initializing when you run the removal software

In the case of A), there is a different way to use the Malware removal software which I will get to shortly. In the case of B), you can typically download Malware removal software and run it and I will cover both of these shortly.

**IMPORTANT:** Two points I need to make here. First if you feel uncomfortable about following any of these steps, please contact a Techie person to handle this for you. We at CCAR may be able to help you as well. Secondly, rare is the case where you or a Techie will run a Malware scan with the Malware removal software and the after-effect is a system that no longer boots. In the 10 years I have been removing Malware, I have had only 1-2 cases out of hundreds where I had to recover an unbootable system which I was able to do. The reason for this outcome was that the Malware had spread so deep into the system that it infected boot files.

So my advice is that even though the odds are very slim that you will have a system that is worse than it was before the Malware removal process, as long as you can operate your system, you should back up your files to an external hard drive or USB flash drive before proceeding.

Please make sure you have read all the previous information prior to this part before proceeding.

## **THE FIX**

If you are:

### **A) Your system is incapacitated and you literally cannot do anything**

You will need to follow these steps:

First, turn off your computer and turn it back on and right when you turn it back on, tap the F8 key once every 1-2 seconds until you see a black screen with white text. This screen indicates boot options. You will want to choose the option that says "Safe Mode with Networking". When you login this way, your display will show big icons and everything will look oversized. That's expected.

When you get to the desktop, you will want to attempt to go to the Malware removal software site of your choice (a few listed below) and download the software. If your browser does not work, the other option is to locate and use another computer and download the software on that computer to a USB flash drive and then plug the drive into the infected computer and run the Malware removal software as in the following.

**From this point going forward, the instructions apply to both:**

**A) Your system is incapacitated and you literally cannot do anything**

*And you are logged in to Safe Mode with Networking*

Or....

**B) Your system is simply behaving oddly and you can't put your finger on it**

*And you are logged in normally*

I can now assume you have downloaded, installed, and updated your new Malware removal software and are ready to run it.

Here is what you want to do. There are typically two options for scanning your system with Malware and they have different names but one is a quick scan and the other is a full scan. A quick scan option covers the most commonly infected files. Some removal software programs don't have this choice and you will have one scan mode. If you do have the choice, choose the one that looks to perform a full scan. The scanning process can take up to an hour or more depending on how many files your computer has.

At the conclusion of the scan you will see a results window and will want to click on it. There is usually a button that says "Remove Selected Items". You will want to choose this. After the process is complete, it may ask you to reboot. At the point of reboot, it is possible you may then be free of Malware. If you feel that you would like to be extra sure, you can always install a second Malware removal software program, such as from the list at the bottom.

Now I am going to list the free software that I have used over the years that has worked very well for me. My favorite lately has been Malwarebytes. I usually install 1-2 Malware removal programs because they often overlap in their effectiveness.

Below is the list of software I have used in order of favorites. My personal recommendation is to just use Malwarebytes to see if that will result in success for you, and then move on to one of the others. I would recommend having no more than 2 Malware removal programs on your system.

**IMPORTANT:** I don't recommend doing a typical search through a search engine for Malware removal programs because you may instead get Malware cloaked as a removal program. Always refer to a Techie person or Tech magazine to learn the best removal programs, such as the list below.

Note: The free versions have been very effective from my observations. Free versions usually have a link somewhere on the page of the sites below.

Again, as noted, if you feel uncomfortable using any of this software, please contact a Techie or perhaps we can help.

So without further preamble.....

**MALWAREBYTES:**

<http://malwarebytes.org>

**SUPERANTISPYWARE:**

<http://superantispyware.com>

**CCLEANER:**

<http://www.ccleaner.com>

**SPYBOT SEARCH & DESTROY**

<http://www.safer-networking.org/en/index.html>

Here's to happy Malware-free computing!

Richard Tausch, MCSE, CCNA, CompTia Security +