JK Computer Solutions, Inc. tip on how to avoid malware

There are several simple steps that can assist you in avoiding a malware infection.

1.) **Keep the following programs up to date at ALL times:**
   a. Adobe Reader – http://get.adobe.com/reader/
   b. Adobe Flash – http://get.adobe.com/flashplayer/ (make sure to visit this with each of your browsers, Internet Explorer, Firefox, Chrome, etc.)
   c. Java (most important) – http://www.java.com/getjava/

2.) **Keep a valid anti-virus product running on your system.**
   a. We recommend Kaspersky Anti-Virus which we sell directly to you if requested.
   b. A less effective free option is Microsoft Security Essentials.

3.) **Use a browser which can block scripts from running on a web page**. Scripts are essentially mini-programs that web pages have you run in order to show advanced content. Most attacks on web pages come in through scripts. We recommend using FireFox with the NoScript addon.
   a. FireFox – www.mozilla.org/en-US/firefox/
   b. NoScript – https://addons.mozilla.org/en-US/firefox/addon/noscript/

4.) **Be aware that if it's free, they're making money from you somehow**. If it's a free download they are either making money advertising to you, making money by installing programs that track your computer usages (for advertising), or are trying to install something malicious to draw money directly from you either through theft or misinformation.

5.) **Do NOT use programs that offer to speed up your system.** They simply will not work and likely will install spyware, adware, and/or viruses. Registry cleaners do not work, registry optimizers do not work, boot time improvement software does not work, etc. If we found one we'd be using it and we haven't found a program yet that will offer more than a few % improvement in boot times/performance.

6.) **Realize that allowing a program to run on your computer gives it as much control over your computer as you have.**

Information about malware removals: Due to the ever changing nature of malware and other virus type programs, removal can never be 100% guaranteed. Certain artifacts might remain in the operating system even after the infection itself has been removed including but not limited to: network instability, operating system instability, and specific program instability. Also, due to the malware needing to be identified by anti-virus/anti-malware vendors before it can be removed there remains the possibility that not all infected items will be removed. Additional time may be required to resolve issues not found during the initial virus/malware removal.