One of the most common questions found when cleaning Spyware or other Malware is "how did my machine get infected?". There are a variety of reasons, but the most common ones are that you are not practicing **Safe Internet**, you are not running the proper security software, and that your computer's security settings are set too low.

Below I have outlined a series of categories that outline how you can increase the security of your computer so that you will not be infected again in the future.

Practice Safe Internet

One of the main reasons people get infected in the first place is that they are not practicing Safe Internet. You practice Safe Internet when you educate yourself on how to properly use the Internet through the use of security tools and good practice. Knowing how you can get infected and what types of files and sites to avoid will be the most crucial step in keeping your computer malware free. The reality is that the majority of people who are infected with malware are ones who click on things they shouldn't be clicking on. Whether these things are files or sites it doesn't really matter. If something is out to get you, and you click on it, it most likely will. Below are a list of simple precautions to take to keep your computer clean and running securely:

1. If you receive an attachment from someone you do not know, **DO NOT OPEN IT!** Simple as that. Opening attachments from people you do not know is a very common method for viruses or worms to infect your computer.

2. If you receive an attachment and it ends with a **.exe**, **.com**, **.bat**, or **.pif** do not open the attachment unless you know for a **fact** that it is clean. For the casual computer user, you will almost never receive a valid attachment of this type.

3. If you receive an attachment from someone you know, and it looks suspicious, then it probably is. The email could be from someone you know infected with a malware that is trying to infect everyone in their address book.

4. If you are browsing the Internet and a popup appears saying that you are infected, **ignore it!** These are, as far as I am concerned, scams that are being used to scare you into purchasing a piece of software.
   There are also programs that disguise themselves as Anti-Spyware or security products but are instead scams.

5. Another tactic to fool you on the web is when a site displays a popup that looks like a normal Windows message or alert. When you click on them, though, they instead bring you to another site that is trying to push a product on you. We suggest that you close these windows by clicking on the **X** instead of the OK button. Alternatively, you can check to see if it's a real alert by right-clicking on the window. If there is a menu that comes up saying **Add to Favorites...** you know it's a fake.

6. Do not go to adult sites. I know this may bother some of you, but the fact is that a large amount of malware is pushed through these types of sites. I am not saying all adult sites do this, but a lot do.

7. When using an Instant Messaging program be cautious about clicking on links people send to you. It is not uncommon for infections to send a message to everyone in the infected person's contact list that contains a link to an infection. Instead when you receive a message that contains a link, message back to the person asking if it is legit before you click on it.

8. Stay away from Warez and Crack sites! In addition to the obvious copyright issues, the downloads from these sites are typically overrun with infections.

9. Be careful of what you download off of web sites and Peer-2-Peer networks. Some sites disguise malware as legitimate software to trick you into installing them and Peer-2-Peer networks are crawling with it. If you want to download a piece of software a from a site, and are not sure if they are legitimate, you can use McAfee Siteadvisor to look up info on the site.

10. **DO NOT INSTALL** any software without first reading the End User License Agreement, otherwise known as the EULA. A tactic that some developers use is to offer their software for free, but have spyware and other programs you do not want bundled with it. This is where they make their money. By reading the agreement there is a good chance you can spot this and not install the software.

Visit Microsoft's Windows Update Site Frequently

It is important that you visit http://www.windowsupdate.com regularly. This will ensure your computer has always the latest security updates available installed on your computer. If there are new updates to install, install them immediately, reboot your computer, and revisit the site until there are no more critical updates.

Make Internet Explorer More Secure

1. From within Internet Explorer click on the **Tools** menu and then click on **Options**.
2. Click once on the **Security** tab
3. Click once on the **Internet** icon so it becomes highlighted.
4. Click once on the **Custom Level** button.

    a. Change the **Download signed ActiveX controls** to **Prompt**

    b. Change the **Download unsigned ActiveX controls** to **Disable**

    c. Change the **Initialize and script ActiveX controls not marked as safe** to **Disable**

    d. Change the **Installation of desktop items** to **Prompt**

    e. Change the **Launching programs and files in an IFRAME** to **Prompt**

    f. Change the **Navigate sub-frames across different domains** to **Prompt**

    g. When all these settings have been made, click on the **OK** button.

    h. If it prompts you as to whether or not you want to save the settings, press the **Yes** button.

5. Next press the **Apply** button and then the **OK** to exit the Internet Properties page.

Use an AntiVirus Software

It is very important that your computer has an anti-virus software running on your machine. This alone can save you a lot of trouble with malware in the future.

Update your AntiVirus Software

It is imperative that you update your Antivirus software at least once a week (Even more if you wish). If you do not update your antivirus software then it will not be able to catch any of the new variants that may come out. If you use a commercial antivirus program you must make sure you keep renewing your subscription. Otherwise, once your subscription runs out, you may not be able to update the programs virus definitions.

Make sure your applications have all of their updates

It is also possible for other programs on your computer to have security vulnerability that can allow malware to infect you. Therefore, it is also a good idea to check for the latest versions of commonly installed applications that are regularly patched to fix vulnerabilities. You can check these by visiting **Secunia Software Inspector** and **Calendar of Updates.**

Use a Firewall

I can not stress how important it is that you use a Firewall on your computer. Without a firewall your computer is susceptible to being hacked and taken over. I am very serious about this and see it happen almost every day with my clients. Simply using a Firewall in its default configuration can lower your risk greatly.

Install an AntiSpyware Program

Recommended, and free, AntiSpyware programs are Malwarebytes Anti-Malware, SpywareDoctor (free in the GooglePack), SuperAntiSpyware, Spybot - Search and Destroy, and Ad-Aware Personal.

Installing these programs will provide spyware & hijacker protection on your computer alongside your virus protection. You should scan your computer with an AntiSpyware program on a regular basis just as you would an antivirus software.

Install SpywareBlaster

SpywareBlaster will added a large list of programs and sites into your Internet Explorer settings that will protect you from running and downloading known malicious programs.

Update all these programs regularly

Make sure you update all the programs I have listed regularly. Without regular updates you **WILL NOT** be protected when new malicious programs are released.

Follow this list and your potential for being infected again will reduce dramatically.