Providing the Support and Products
to Keep YOUR Business Up and Running

3003 N Joplin St, Pittsburg, KS 66762, Phone: ***855-835-8434***

2012 May

To my clients:

RE: **Tips to avoid getting infected by a Virus or Spyware**

Much of my business comes from cleaning computers infected by viruses. As one of my valued clients, I want to encourage you to use the internet safely. Below are guidelines that have been developed with a group of my colleagues from around the world.

1. Install an Anti-Virus/Anti-Spyware program. Be sure to keep this up to date and do weekly full scans. While there are many good products available, I currently carry and recommend Kaspersky Anti-Virus and Malwarebytes (anti-spyware). (Run only one anti-virus program)
2. Set up your Windows Update to automatically download patches and upgrades. This will allow your computer to automatically download any updates to both the operating system (i.e. Windows) and Internet Explorer. These updates fix security holes in both pieces of software.
3. Install and use an alternative web browser such as "Firefox," "Opera," or "Google chrome" which generally poses less of a security risk.
    a. For more information on this see: http://www.the-rescue-tech.com/about/computerlinks.html
4. Visit http://www.mywot.com/ and install this tool in your browser. It is a social rating system that can give you a warning about a site as you are browsing the net. Take time to read how it works, as it has some limitations, but can be very helpful while you surf.
5. If you use "FireFox", I recommend the add-ons "NoScript" and "Flash Block", however, these are somewhat advanced tools, so I don't recommend them for everyone.
    a. If you use "Chrome", I recommend the extensions "ScriptNo" and "FlashBlock"

Doing the above is the basic minimum that you should do to help protect your computer;
HOWEVER, they will not guarantee 100% protection.
To further reduce the possibility of getting a virus or other malware, please read the following advice:

1. **Email is a common way of getting infected.**
   While you can safely open an Email, NEVER click on a link within it or open an attachment that you are not positive is from a trusted source.
   Here are 2 scenarios:
    a. **You get an Email from someone you DON'T know.** You open it. It tells you (or, persuades you) to click on a link in the Email. You do so. That is when you get infected.

CompTIA Network+ CERTIFIED CompTIA A+ CERTIFIED
E-mail: bill@the-rescue-tech.com http://www.the-Rescue-Tech.com

Frequently, the Email appears to be from a bank or a company you know. Do not fall for this. Businesses do not normally send unsolicited Email.

   b. **You get (what appears to be) an Email from someone you DO know.** Unknown to you, a virus generated that Email (and not your friend). It could be that your friend's computer is infected, but, not always. Obviously, the actual Email writer doesn't know you and cannot say anything personal to you, so, typically, it says something like "Click on this link for some important information... ". You are now infected.
   c. **If in doubt, delete the Email.**

2. **Social Networking (Facebook, etc.)**
   Social Networking has become VERY popular, and hackers have taken notice of this. Take GREAT care in the links you click on and try to keep the applications for these sites to a minimum. They can affect your computer's performance, or worse, can also be a malware package in disguise.
3. **Instant messengers.**
   The same caution should be used with opening links and attachments as Emails.
4. **Web sites (Anything popular)**
   a. Visiting Adult (i.e. Pornography), Free game or gambling sites pose a high risk of infection.
   b. Use caution on social networking sites. Do not download software or "Addons" from web sites that you are unfamiliar with. This includes sites such as "Facebook", etc.
   c. Games of all kinds have become a target of hackers.
   d. Coupon sites have also gotten the attention of hackers.
5. **Do not click on sudden pop-up windows** while browsing the internet.
6. **Do not use disks or USB drives that other people give you.**
   They could be infected with a virus. Of course, you can run a virus scan on it first, but Anti-Virus programs are not 100% effective.
7. **Stay away from file-sharing sites.**
   Sites that distribute illegal software, music, or movies are known to be riddled with viruses. This includes torrents or other forms of P2P activities (Limewire for example). Staying away from these sites and programs is best for your computer's health, as well as a good way to avoid being sued for copyright violation.

The above advice is generally good practice to follow but is not a 100% guarantee that your computer will not get infected again in the future. However, by following these tips you minimize the possibility greatly.

Be wise and careful as you surf the internet.

Sincerely,

Bill Emmerling, Technician, CompTIA A+
bill@the-Rescue-Tech.com
Toll Free: 855-835-8434, 620-308-6448