How to limit your risk of Spyware and Virus infection on a Windows System.

Brought to you by SES Consultants

There are many possible ways your computer can become infected with Spyware or a virus. In this white paper, we will discuss the three most common routes of infection and what steps you can take to minimalize this risk to you.

1. Unsafe internet sites or browsing habits.

Possible routes of infection include:

- **Infected web page**

Some websites can become infected due to the host's system being infected, spreading the infection to you.

- **Hacked web page**

Some website can be compromised and try to force you to download software or popups that use software built in to Windows to infect your computer

- **Deliberately dangerous site**

Some websites on the internet are created to infect or compromise your computer to allow unauthorized access to your system

- **Spoof sites**

Some seemingly valid sites that appear to be the correct site you are searching for can actually be cloned sites to harvest your personal information.

2. Unsafe downloads

Possible routes of infection include:

- **Bundled software**

Many free software offered on the internet is marketed as free. Often this software has bundled with other companies that have bundled freebies during the install

- **Unsafe source**

Some sources are more risky than others. Files called torrents can be infected for the purpose to steal your identity, data or to ransom your computer.

- **Demo software**

Many times companies offer their product for a limited trial. This software may appear to be valid but actually compromising your system.

3. File sharing

Possible routes of infection include:

- **Friends system is infected**

Sharing files between you and a infected computer can lead to your system being infected.

- **P2P**

Peer 2 Peer sites are a hotbed of infected files. Services like Limewire, Bittorrent and bearshare can pass infections to your computer.

- **Web based sharing**

Several sites on the internet offer free storage to share your files with others. These sites can become compromised and infect your computer.

So, what can you do to minimize your risks to infection?

Here is our advise:

1. **Change your behavior**
2. **Change your browser**
3. **Use tools to prevent infection**
4. **Updates, updates and more updates**

1. Change you behavior:

If you put your hand on the oven and get burned, you learn to avoid the hot surface of your oven. If your friend tells you to avoid a restaurant, you think twice about eating there. This also applies to your on-line habits.

To avoid an infection you need to avoid sites that are risky. Before you visit or download, use a tool like Google.com to search information about the software or website. When in doubt—get out.

Use legit and legal sites to obtain your software or music. This is a simple concept. If you go to a loan shark, do you think you are taking the safest path? Same for software and websites.

Treat the online world a city and avoid the parts that seem too good to be true or risky.

2. Change your browser

What do I mean by change your browser? Well studies have shown the most risky internet browser is Internet Explorer. It comes on all Windows computers and therefor hackers like to target this program. Don't make it easy to become a victim. We highly recommend a browser like Firefox or Chrome. Less malware and virus are written for these browsers.

Make sure you have scripts ad JavaScript off unless you are really sure you need these services on. Java is the #1 most common path of infections from a browser.

Use secure sites when browsing. They often begin with HTTPS and you should see 🔒 in the search bar.

3. Use tools to prevent infection:

This is a big one here people. You need a good anti-virus that offers spyware protection. Don't rely on free products—they are free for a reason. Would you visit a free doctor on the street corner to have your appendix removed? I didn't think so. Same applies to your computer. We, personally, recommend ESET Anti-Virus.

There are other great programs out there, but mixed with other programs that are dangerous to download. Selecting a trustworthy software company is a priority. Visit our website for a list of recommended tools. We update this list as new tools develop.

4. Updates, Updates and more updates:

I can't stress this enough: Update your software, and not just Microsoft Windows. Keep your Windows, Java, browser and any other programs you have installed updated. This includes keeping your anti-virus updated as well. When you update your system you make it harder for older spyware and virus to infect your system.

It's important to remember that even the most protected system still can be infected. When your facing an infection, remember that if your infection is not corrected properly, you can become re-infected and lose data. When facing an infection it is critical that you call a professional to make sure your infection has been removed and your data is secure.

About the Author:

Scott Safford the owner of SES Consultants based in Toledo, Ohio; has been working in Information Technology for over fifteen years. He has worked as both a System Administrator and Network Administrator, as well as a contractor for several well known companies.

Visit Scott's company website at http://sesconsultants.yolasite.com

ALL PC AND APPLE COMPUTERS REPAIRED

Computer Network Support

Slow Speeds Fixed * Virus / Spyware Removed * Training on Windows or Apple

All Brands serviced * After hour service available * In home service or pick up / drop off

Servicing Toledo and surrounding areas

567-343-1731   sesconsulttoledo@gmail.com