INDYLAPTOPS
10411 N. College Ave. Suite 1 • Indianapolis, IN 46280 • 317.844.9495 • www.IndyLaptops.com

Welcome To Different. Welcome to IndyLaptops.

Steps to Help Protect Your Computer from Virus, Spyware and Malware Infections

About Virus, Spyware and Malware Infections

A computer **Virus** is a malicious software program that is capable of causing great harm to your personal files, Operating System or other programs on your computer. A virus can replicate itself and spread from one computer to another via the internet or shared files. The term "virus" is commonly, but erroneously, used to refer to other types of malicious software, including but not limited to spyware and malware. **Malware**, is software used or created by hackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. **Spyware** is a type of malicious software installed on computers that collects information about users without their knowledge. The presence of spyware is typically hidden from the user and can be difficult to detect.

Things You Can Do To Help Avoid Virus, Spyware and Malware Infections

Infections take advantage of technical vulnerabilities and human behavior to find their way onto personal computers. While nothing can guarantee absolute security, the following steps can reduce your computer's exposure to infection.

1. Install and update security software

Anti-virus, anti-spyware, and other similar products can be useful to detect, stop, and remove infections that have found a way onto your computer. IndyLaptops recommends Norton Internet Security for the most comprehensive protection. Look for a product that:

- Can protect against both known and unknown viruses, spyware, and malware in real time.
- Includes automatic updates and Scheduled Scans.
- Has been reviewed in established publications and/or tested by independent labs.

2. Secure your operating system

Your operating system (e.g., Windows XP, Windows Vista, and Windows 7) plays a central role in managing the security of your computer. Keep it safe by:

- Installing security updates as they become available
- Using a built-in or third-party firewall

3. Keep your computer software up to date

Keeping your Operating System updated is critical, but it's equally important to keep your web browser and plug-ins, Security software, and other applications up to date to patch "holes" that can allow infections into your computer.

- Most software, including Windows, has an automatic update feature - ***Do Not Ignore These Updates***.
- For software that doesn't have such a feature, look in the menus (especially the "help" menu) for a manual "check for updates" option.
- Adobe Flash Player and Java by Oracle are used on many websites. It's important to install any available updates for these plug-ins. To be sure you're receiving genuine updates, please visit the websites listed below.
- For Adobe Flash Player visit: http://get.adobe.com/flashplayer
- For Java updates visit: http://java.com/en/download/index.jsp

-OVER-

4. Remove or disable high-risk or unnecessary applications

Using an internet file sharing site or service such as a torrent site puts you at high-risk for an infection. We recommend avoiding such sites. If you use a toolbar add-on such as a search bar, use only trusted brands like Google, Yahoo, Microsoft, etc. If it's something you're unsure of, it's best to research the add-on or just avoid installing it.

- Do not use internet file sharing sites or services such as torrent sites.
- Uninstall toolbars, plug-ins, and other software that you don't use or are unsure of.

5. Always use caution

Malicious software distributors are always looking for new ways to deceive users into installing their software. Here are a few more tips to avoid being infected:

- Always read the safety guides on Social Networking sites such as Facebook. Facebook has a very good safety guide. You can find it at http://www.facebook.com/help/safety. Other Social Networking sites have similar safety guides. Take the time to read these guides to help protect yourself from infections and identity theft.
- Avoid opening email attachments or downloaded files unless you can verify that they came from a reputable/known source.
- Be wary of clicking links in email messages. It may be safer to visit the site by typing its URL in to your browser or, if applicable, using an existing shortcut that you have to the site.
- Be alert to fake virus warnings, often within web browser windows, that encourage you to download, install, or purchase unfamiliar software.
- Pay attention to warnings from web browsers, search engines, and security products that try to protect you from known or suspected threats.

Remember, using your computer on the internet is much like driving your car on a busy highway. When you're on the road you're at risk and the same goes for when you're on the internet. It's important to be cautious and use common sense. And in both cases, it never hurts to stop and ask for directions. That's what we're here for, so always feel free to call for advice.

INDYLAPTOPS
10411 N. College Ave. Suite 1 ● Indianapolis, IN 46280 ● 317.844.9495 ● www.IndyLaptops.com

Welcome To Different. Welcome to IndyLaptops.

This document, along with other helpful Tips and Support documents, can be found on our website in electronic PDF format at www.IndyLaptops.com/support