5 Things to Do as Soon as You Purchase a New Computer

SUMMARY: Increase your computer security and reduce potential headaches later by doing these five things as soon as you purchase a new computer.

Have you just purchased a new desktop or laptop computer? Congratulations, and hopefully you will get plenty of use out of your new machine, whether it is for business, finance, research, multimedia, or purely entertainment (or a little of all the above).

But wait - don't open the boxes, plug in the cords, and try to start surfing the Internet just yet! Take a few minutes and follow these 5 steps that can help increase your computer security and possibly remove some potential headaches down the road.

1. Emergency Disks

Some computers come packaged with CDs or DVDs you can use to reinstall the operating system and pre-installed software in case something goes wrong, such as a hard drive hiccup, malware infestation, or an itchy trigger finger that loves pressing the '*Del*' key. If such discs are included, place them in a safe place and make copies once the computer is set up.

If these did not come with your computer, read its manual for instructions on how to create them, if possible. Do so ASAP - before you go online, install new software, uninstall software that came pre-packaged but you do not need, etc. Better yet, make a second copy of these disks for safe keeping.

2. Install Security Software

Before connecting to the Internet, either via a wired or Wi-Fi connection, make sure you have a working firewall and antivirus software at a BARE minimum; surfing without such programs can open your computer up to all types of nasty malware. If your operating system has a built-in firewall, turn this on if nothing else is available, but do consider downloading a replacement.

If you have another computer, use it to download a firewall, anti-virus, and anti-malware applications. Either burn a CD/DVD or use a USB flash drive to copy them to the new machine. Install this software **before** you ever connect to the Internet to reduce the chances of problems. Once you are online, immediately download updates as needed.

Note that if your computer comes built-in with security software, you may need to remove these packages first if you decide to install alternatives (see below).

3. Uninstall Software

Go through the list of installed software through the computer's "Add/Remove Programs", "Uninstall or change a program", or similar tool (check the Control Panel). Remove any pre-installed "bloatware", software you may not need such as trial games, photo applications you may never use, website toolbars, links to Internet Service Providers you will never access (especially if you already have one), etc. Do keep the installed security software unless you are offline and ready to install different applications.

4. Consider a New Web Browser

When you go online, you are not stuck with your operating system's default web browser if you want to surf the web. There are plenty of alternatives available such as Mozilla Firefox, Opera, and Google Chrome, and using another web browser may increase your overall security.

Even if you install a new web browser, be sure to keep the one that came with your operating system up-to-date to help prevent malware from attacking your system via an exploit.

5. Update All Software

Speaking of doing software updates, after going online but before browsing the web, **immediately** update your operating system (including the built-in web browser). Check for updates to document readers such as Adobe Acrobat Reader and any installed multimedia players. Plus, look for updates to installed browser plug-ins such as Adobe Flash, Adobe Shockwave, Java, QuickTime, and RealPlayer. Exploits can potentially

be found in any software installed on your system; keeping everything up-to- date helps reduce the risk of your computer getting infected by malware.

While you may immediately be ready to unpack and use your new computer, following these five steps will help increase your security when going online. Create or find emergency recovery discs and store them in a safe place in case 'stuff' happens. Install security software such as firewall, antivirus, and anti- spyware applications before you connect to the Internet. Remove unneeded "bloatware" and consider installing an alternate web browser. Finally, before general web surfing or other activities, ensure your operating system and all installed software are up-to-date. By performing these steps, you can start your computer off right, blocking malware and operating well for hopefully years to come.