10 things you should do to a new PC before connecting it to the Internet

Version 1.0
September 29, 2005

By Mark W. Kaelin

Takeaway

A Microsoft Windows PC that has not been updated for security vulnerabilities will be compromised by some from of malware within minutes of connecting to the Internet. Take steps to protect yourself before you start Web surfing.

Table of Contents

10 THINGS......1

1. MAKE A STARTER CD-ROM......2
2. REMOVE THE PROMOTIONAL APPS......2
3. INSTALL ANTIVIRUS SOFTWARE......2
4. TURN ON A SOFTWARE FIREWALL......2
5. INSTALL PRINTERS AND OTHER PERIPHERALS......2
6. ESTABLISH A PASSWORD FOR THE ADMINISTRATOR ACCOUNT......2
7. CREATE A NEW USER ACCOUNT WITH PASSWORD......3
8. TURN OFF UNNECESSARY WINDOWS SERVICES......3
9. ESTABLISH A SYSTEM RESTORE POINT......3
10. INSTALL AND CONFIGURE A ROUTER......3

ADDITIONAL RESOURCES......4

Version history......4
Tell us what you think......4

10 things

It is only natural, when you get a brand new PC, especially one with broadband capabilities built-in, you want to connect to the Internet and see it action. For many, the browser and the World Wide Web are the "killer-apps" of the modern PC—the Internet is what you have a PC for, everything else is just extra fluff.

However, connecting to the Internet with a new unprotected and unpatched PC is practically inviting the nefarious and malicious to infect your PC. According to research published by Sophos in July 2005, there is about a 50 percent chance that an unpatched PC will be infected with malicious software within 12 minutes of connecting to the Internet. Once infected, it is almost impossible to get a PC clean again without completely re-installing the operating system. (We are restricting this conversation to Windows PCs for the moment.)

To prevent the frustration that comes with re-installing Windows, you should take the necessary steps to update, configure, and patch your new PC. Keep in mind that no matter how new your PC is, it will most likely need patching and it will definitely need to be properly configured. Here are 10 basic things you should do before attaching the Internet to a new PC.

1. Make a starter CD-ROM

Before you disconnect your old computer, take a few minutes to burn a starter CD-ROM that contains the latest version of your favorite anti-virus software. I prefer to keep this simple and inexpensive by using AVG from Grisoft, but if you like Norton or McAfee those will work just as well.

To save time later, you should put other security applications on this disk like Spybot Search & Destroy, AdAware, etc. It would also be a good idea to include any updated drivers you might need—drivers for your video card for example. Just like Windows, your video card drivers are likely to be a little old also. You should also put drivers on this disk for peripherals that you will be connecting to your new PC, like cameras, scanners, printers, and game interface devices. Having all of these device drivers residing on a single CD-ROM means you will not have to go to the Internet to retrieve them as you set up your new PC.

2. Remove the promotional apps

After going through the initial setup process where Windows identifies devices you may be asked to register and/or activate you copy of the Windows operating system—hold off on that for now, you can always do that later. This first thing to do is to clean up the mess that shipped in your PC. You should remove all of the promotional and trial software that you do not intend to use from your new PC. This is usually the first thing I do, because invariably one of those apps will ask if I want to activate it or register it—a process that usually involves accessing the Internet. (Some times they don't ask—they just assume I want them on my pristine PC). At this point you should have no connection to the Internet at all, wireless or not.

The applications to be deleted are usually ISPs advertisements like AOL and Earthlink, an antivirus app from a competitor of your current application (something you should already have ready on your CD-ROM), trial versions of Money or Quickbooks, etc. If you are not going to use these, go to the Add/Remove Programs applet in the Control Panel and remove them completely.

3. Install antivirus software

Install the antivirus software that you burned onto a CD-ROM in step 1. The assumption is that any PC purchased after this document is published will have Windows XP SP2 installed, but if SP2 is not installed, you could have that update ready on your disk too. In fact, if you know how, you could have some of the more important Windows patches and updates on your disk also. This would be a good time to install anti-spyware software too.

4. Turn on a software firewall

Windows XP SP2 comes with a modest but still useful software firewall. Before you start surfing the Internet you should turn it on—or you can install an alternative third-party software firewall like Zone Alarm. Any alternative firewalls should have been included on the startup CD-ROM you made in Step 1.

5. Install printers and other peripherals

Before you connect to the Internet it is a good idea to install your other peripherals to your new PC. Performing this step means that when you do connect to the Windows update page, it will see your devices and make suggestions for new Microsoft-tested (WHQL) drivers if they are available.

6. Establish a password for the administrator account

One of the most glaring security vulnerabilities in any new Windows-based PC is that it ships with a wide open administrator access to the root directory. You never want anyone but you to have unfettered access to the admin settings on your PC. And while a password could easily be bypassed by a skilled cracker, it will deter the less determined intruder.

7. Create a new user account with password

This is almost as equally important as password protecting your administrator account. For general day-to-day activities, you do not want to be using your admin account. Instead, you should be using a user account that is also password protected (a password that is different than the one you are using for the admin account, please). This adds another layer of protection for your new PC because a user account does not have the same all-access permissions as an admin account. In some cases, malicious software will be thwarted by this level of permissions restriction alone.

8. Turn off unnecessary Windows services

Microsoft has been doing a better job of this with the release of SP2, but there are still numerous unnecessary Windows services and processes running by default on most PCs. If you'd like to see how many there are just perform the three finger salute (CTRL-ALT-Delete) click Task Manager and then the Processes tab. All of those applications, services, processes, etc. are operating in the background on your PC. The problem is that many can actually open access to your PC to the outside world without your knowledge or active consent. That access is usually justified for what the process is supposed to be doing, it is just that many times your PC doesn't need that process at all—Web servers, network messengers, debuggers—are all processes you probably don't need on your personal PC. (Check out this TechRepublic download for an in-depth examination of these services and for some suggestions for which can be deactivated.)

9. Establish a system restore point

Now that you have performed the first eight steps you should take a moment to establish a system restore point. To manually create a Restore Point, you launch the System Restore utility by clicking Start | All Programs | Accessories | System Tools | System Restore and then follow the steps in the wizard. This step will establish a fall back point if something happens to go haywire later.

10. Install and configure a router

This last step may seem like an unnecessary added expense to some, but in this age of viruses, worms, and other nasty Internet infections, a router standing between you and the outside world coming at you at broadband speeds offers another significant layer of protection. Connecting a PC directly to the Internet means that PC gets its own IP address, which means it can be seen by every sleazebag with malicious intent. By adding a router to your broadband setup, the router gets the visible IP address and gives your new PC an internal address. In addition, routers have hardware firewalls and other features that help block the bad guys before they get to your new PC.

This is especially helpful because the first thing you should do when you do actually connect to the Internet is head directly for Windows Update. This is the most important tip in this guide—the only place you should be heading on the Web when you first connect you PC to the Internet is the Windows Update page. You will not have time to check movie times or football scores. The 12 minute countdown to possible infection starts as soon as you connect.

Additional resources

- **Subscribe to TechRepublic's Downloads RSS Feed** XML
- Sign up for TechRepublic's Downloads Weekly Update newsletter
- Sign up for TechRepublic's Windows XP newsletter
- Check out all of TechRepublic's free newsletters
- 10 PowerToys that complete the Windows toolset and save you precious time
- 50+ keyboard shortcuts for moving faster in Windows XP
- Take control of Windows XP system properties during both startup and shutdown

Version history

Version: 1.0
Published: September 29, 2005

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to drop us a line and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team