Recognizing a PC with Malware

What can you do if you think your computer is affected by spyware or a virus or other malware? (Malware is short for malicious

What can you do if you think your computer is affected by spyware or a virus or other malware? (Malware is short for malicious

software.) First let me assure you that you aren't in this alone. There are excellent resources and community sites dedicated to

helping dig people out of the mess that malware can make. Many of them are free and I'll point you to them in this column. I'll also

explain how to recognize if your computer has malware running on it and point you to antivirus programs and anti-spyware tools to

help you get rid of it. And I'll describe how to use recovery options that help get your PC back to working the way it's supposed

to. And, finally, I'll talk about "The Last Resort"-rebuilding your PC from scratch.

How to recognize malware
Malware is designed to run undetected in the background. So how can you tell if you have undesirable software on your system? The

signs to look for include:
• Advertising pop-ups that appear every few seconds.
• Extra toolbars in your browser that won't go away.
• Browser going to sites you didn't tell it to go to.
• Browser settings changing so your home page won't open.
• Unexplained system slowdowns.
• Sudden rise in computer crashes.

If you're experiencing these kinds of problems, it's a good idea to treat your PC as if it might be infected by checking it out

thoroughly. Although there are other reasons why your system might slow down or frequently crash, if you're noticing these obvious

indications of malware, your system has probably been compromised. It's time to take defensive action.
Update antivirus programs
The first step in any attempt to repair or recover a compromised PC is to update your defensive tools. Your antivirus or

anti-spyware tools need to be updated to the absolute latest versions and the most recent definition files. If you can do this on

the PC that has the problem, then do it there. If not, you'll need to use another PC to download the latest versions and put them on

a CD or USB drive that you can use to work on the infected PC. I like the USB drive because it's highly portable and easy to update

if you need to. And everything you'll need will fit easily on a 128-MB USB drive.
Gather your original software CDs and disks as well, including your original Windows CD and the Windows XP

Service Pack 2 (SP2) CD.

You may need them before this is over, and it's good to get everything organized and ready before you start. Windows XP SP2 provides

better protection against viruses, hackers, and worms. If you don't have a copy of the Windows XP SP2 CD, you should borrow one from

a friend, order SP2 on a CD, or download the Network Install and copy it to a CD.
If you don't already have an antivirus program running on your computer, you'll find a number of companies offering antivirus

Important: Uninstall any antivirus software you are currently using before installing a new product; having two different programs

might cause problems on your computer.
Typically, these software companies make special offers of free trial versions of their antivirus and firewall packages, which

should be enough to get you through this process. But to help avoid being back in this mess again, you'll want to choose one of them

and get a full subscription to it so you stay up to date.
If you still have good working Internet connectivity, you can also use one of the excellent, free, online virus scanners. My

favorite and one of the best is Panda Software's Panda Free Online Scanner

One of the most annoying and difficult to remove pieces of unwanted software is Cool Web Search and its variants. To remove this,

you're best bet is CWShredder, a dedicated program that just goes after this.
You'll also need a good anti-spyware product that can help you with the detection and removal of spyware or other malware. Here, one

is good and two or more are sometimes better. They don't interfere with each other, generally, and they each seem to have slightly

different strengths. The two I use regularly and recommend are Spybot search & destroy

Microsoft, which is in beta testing now and holds some promise as well. (Beta software is pre-release software that is distributed

for feedback and testing purposes.) The Microsoft product is a security technology that helps you detect and remove known spyware

from your PC. It also helps prevent spyware from getting on your computer in the first place. I've been using it and really like the

way it works, but because it's a beta version, it won't be the right choice for everyone until the final release. For one thing,

Microsoft doesn't provide technical support for beta releases. Although formal support is not offered for this beta, you can go to

the newsgroups to help get your questions answered.
Finally, it's a good idea to have a couple of other programs available. LSPFix and WinSock XP Fix can help restore your Internet

connection if the cleanup process messes that up.

Back up critical files
If you can, now would be a really good time to back up critical files you'd hate to lose. Don't try to back up programs or the

operating system-there's no point since they may be compromised and can be replaced. But those pictures of your daughter's wedding,

your résumé, and your doctoral thesis-those are irreplaceable. Please, copy them somewhere safe, since anything you do to remove

this kind of malicious software is serious and could leave your PC in a state where it might be difficult to recover or save your

critical files.
Where or what you copy them to doesn't really much matter. A CD or DVD if you've got the hardware and software to do that, or a Zip

disk, or just plain old floppy disks will work. But whatever medium you use, having a backup will give you the confidence to attack

this malicious software without fear of losing something critical. Ed Bott's Windows XP Backup Made Easy

Scan and remove
Once you have your defensive programs ready, located your original CDs and DVDs, and made a backup of your critical data files, it's

time to start figuring out exactly what you have on your system that shouldn't be there. But before you start, disable System

Restore. The last thing you'd want to do is restore to this point anyway, and this will prevent versions of the noxious software

from being saved in the restore point.
To disable System Restore
1. Click Start, right-click My Computer, and then click Properties.
2. On the System Restore tab, select the Turn off System Restore box, and click OK.

The first step should be to try the obvious. Use Add/Remove Programs in Control Panel for programs that shouldn't be there and try

to uninstall them first. Some of the annoying adware programs will actually uninstall and stay uninstalled so you might as well get

rid of them first.
Next I scan for conventional viruses. Use the antivirus software that you downloaded and updated or one of the online scanners if

you're still online. Deal with anything it finds, either by deleting or cleaning as appropriate. Microsoft offers a Malicious

Software Removal Tool (http://www.microsoft.com/security/malwareremove/default.mspx) that is updated on the first Tuesday of each

month. This tool checks computers running Windows XP, Windows 2000, and Windows Server 2003 for infections by specific, prevalent

malicious software-including Blaster, Sasser, and Mydoom-and helps remove any infection found. When you're done, it's time to

disconnect from the Internet. Unplug the network connection or disconnect the modem.

Next, run CWShredder. Although it only deals with a single (but pervasive) problem, many of the Cool Web Search variants can prevent

the other anti-spyware programs from doing their job correctly, so it's best to go after this one first.
Now it's time to run the anti-spyware scanners. It doesn't really matter what order you run them in, but be prepared for a fairly

lengthy list of things to deal with. Initially, I'd ignore any that are described as cookies-they're low on our list of concerns for

now. But everything that looks like a program or that they report as a critical issue should be quarantined or deleted.

Running in safe mode
One recommendation that some experts make is to run your antivirus and anti-spyware scans and cleanup in safe mode. Some problems

that can hide from these programs in normal user mode are exposed in safe mode. Other experts disagree and suggest that there is

little difference. I'm of the school that thinks it can't hurt, so I suggest you try running your scans first from a normal boot,

but when you've done all you can from there, start in safe mode and try running the scans again.
To start in safe mode
1. Click Start, click Shut Down, click Restart from the list, and then click OK.
2. While your computer is starting, press the F8 key until the Windows Advanced Options Menu appears.
3. Select Safe Mode and press ENTER as needed.

For more on safe mode and the options available in the Windows Advanced Options Menu, see a Description of the Safe Mode Boot

Options in Windows XP at http://support.microsoft.com/default.aspx?scid=kb;en-us;315222.
Finally, when you're done fixing everything and you think you've got it all, I think it's wise to install or reinstall Windows XP

Service Pack 2. Now turn on Windows Firewall, turn on System Restore, and you can connect your PC back to the Internet. Before you

do anything else, go to the Windows Update site (http://update.microsoft.com) and download all of the latest security fixes. Then,

turn on Automatic Updates to make sure you stay up to date.
Getting help
Removing undesirable software can be a daunting task. But as I said in the beginning, you're not in this alone. There is a wealth

of resources available to you at every stage of the process. I can't begin to list them all, but some that I know about are the

following:
• Microsoft Security Help and Support-the support is free for security problems and getting help removing malware is definitely a

• Microsoft Security Home Users Newsgroup-good place to start, with a wealth of users and MVPs responding to your queries 24 hours a

day: Located at

• Broadband Reports Online Security Community Forum-an excellent resource for really persistent and difficult problems, with help

from Microsoft MVPs and other users: Located at • Spyware Info Forums-excellent help and fast responses: Located at • AumHa Forums-a great resource for a wide variety of Windows problems, run and staffed by Microsoft MVPs: Located at

The last resort
Finally, I want to talk about the last resort, which is performing a clean installation of Windows XP. This is not something to do

casually, since you will certainly lose data and have to re-install all your programs, but it is an option if all else fails.
