Just Like Starting Over

When Should You Reinstall Windows?

You know better, don't you? Some folks think that when their computer catches a virus, starts spewing error messages, or just gets too slow to be useful, they need to buy a whole new PC. Others may be tempted to spend $50 on software that claims to fix all sorts of problems (although our experience with utilities like these has been disappointing at best).

You may know that you can fix many problems your computer has by reinstalling your OS (operating system), such as Windows XP. If you have an installation CD for your OS, or a recovery CD, DVD, or hard drive partition from your PC's manufacturer, you can give your computer a clean bill of health without spending any more than your time. On the other hand, if hardware such as a memory module, power supply, or video card has gone bad, replacing it may save you the trouble of a reinstallation by fixing the root cause of some errors.

Many users keep their systems running well by revamping their OSes every year or two. Windows in particular simply was not designed to run for too many years without a refresh in most cases. Typical Windows installations accumulate problems over the years as users install and remove software and hardware, update drivers, and apply patches to the OS and apps. It pays to clean things out.

It's faster and easier to first try to repair Windows, meaning to attempt to reinstall it without disturbing your applications and personal data files (see the "Step-By-Step Reinstalling Tutorials" section of this issue). However, some problems, such as a bad virus or rootkit infection, mean that only reformatting your hard drive and reinstalling everything—your OS, your applications, and your data—will solve your troubles (we've included guides for this, too, in the "Clean Installation Tutorials" section). Don't forget to read the "Backing Up" section of this issue to learn how to back up all of your personal data and settings before you do anything else.

Tipping Points

Few people really want to spend a weekend reinstalling their OSes, but there are a few common scenarios that should make you seriously consider doing so. Most are listed in the "You Know It's Time To Reinstall When..." sidebar, but a few of those topics merit a little more discussion.

Do over. When Windows Me/XP users get into a bind with new errors or a bad software (un)installation, they often turn to System Restore. This built-in utility can "turn back the clock" on a PC and return it to its state on an earlier date (see "The Way We Were" on page 11 in this issue).
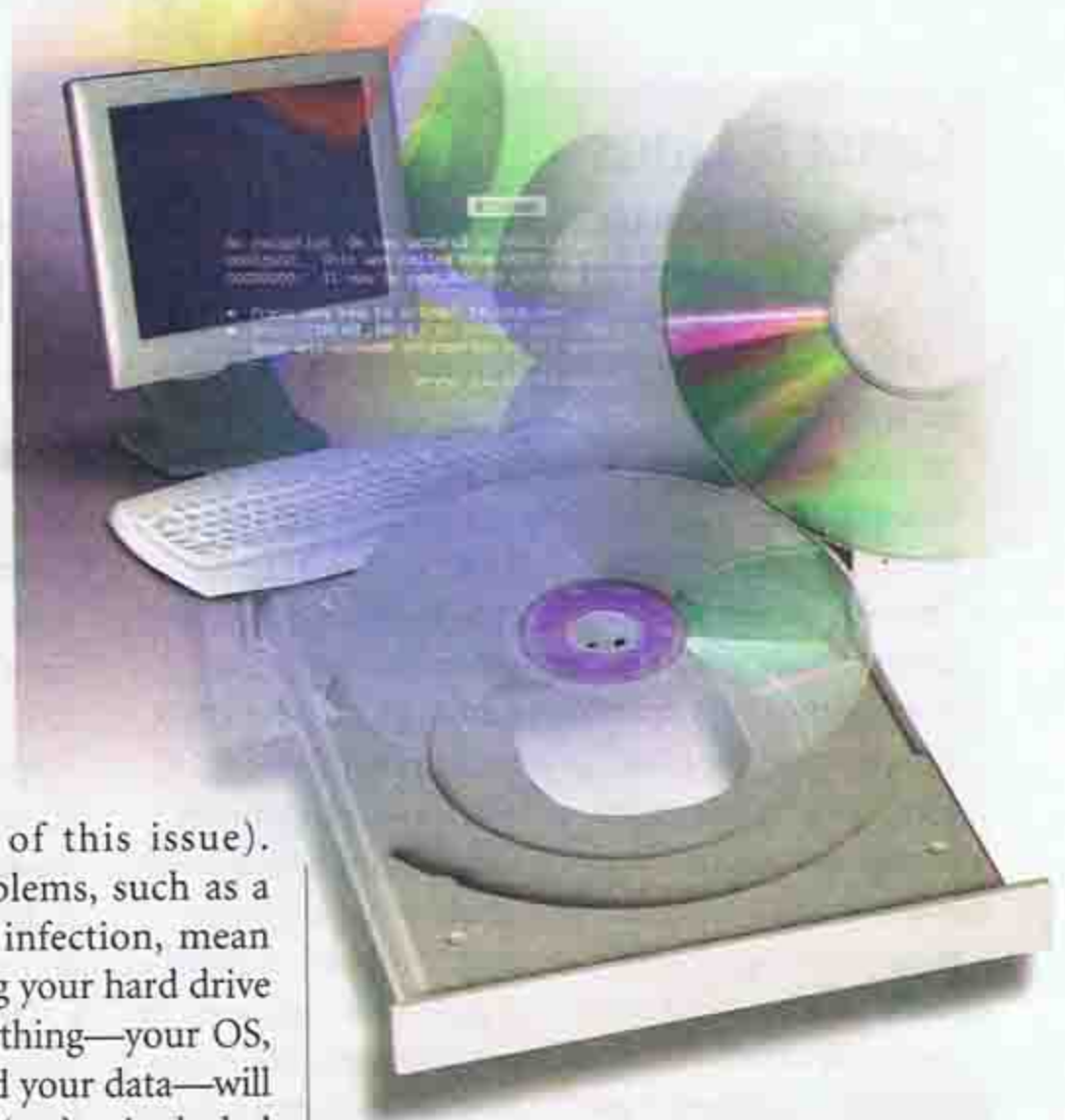
Unfortunately, System Restore can't fix every problem. If the trouble started too long ago, such as a few weeks, Windows may have erased an old pre-error Restore Point (a virtual snapshot of the state of the computer at that moment) to make room for a more recent post-error one. Also, System Restore occasionally can't roll a PC back to a particular Restore Point for one reason or another.

If Windows won't boot at all, you might see a black screen with a list of options, such as Safe Mode, Safe Mode
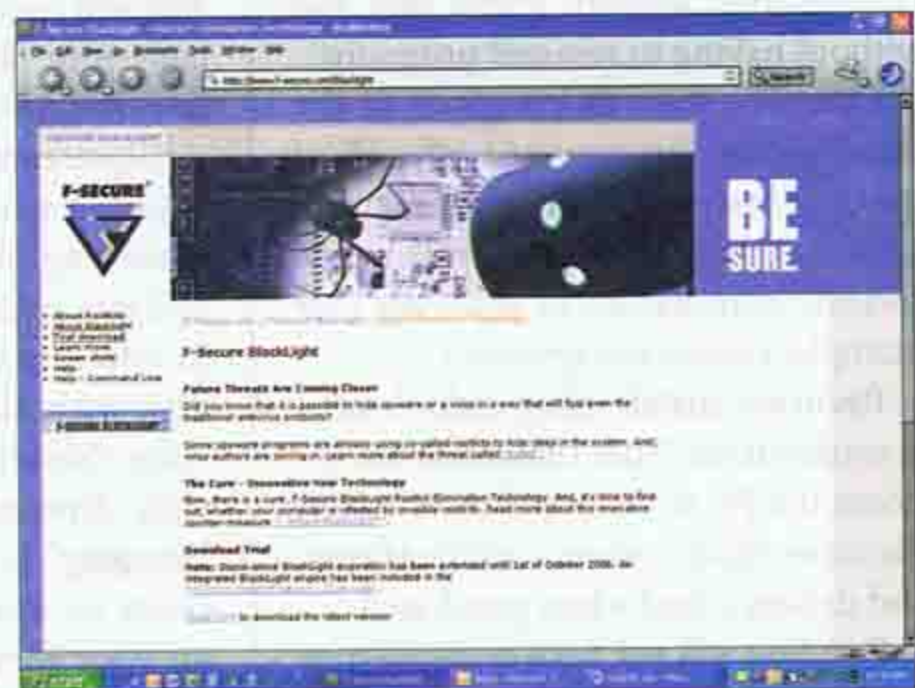
F-Secure's BlackLight (www.f-secure.com/blacklight) can find many rootkits, but in general, experts say that only a reformat and reinstall will get rid of one.

With Networking, and others. If not, try pressing F8 repeatedly after a restart. Select Last Known Good Configuration, which restores Windows' Registry with a backed up version. If this doesn't allow Windows to boot, and you don't suspect that a device problem or recent BIOS (Basic Input/Output System) change is the culprit, an OS reinstallation might be necessary.

Malware. Even if your PC gets infected with a virus, rootkit, worm, or spyware, there's nothing physically wrong with it. It just means there is some very unwanted data on your hard drive.

If your antivirus and antispyware apps (and free tools such as Trend Micro's CWShredder [www.trend micro.com/cwshredder], F-Secure's BlackLight [www.f-secure.com/black light], and Sysinternal's Rootkit Revealer [www.sysinternals.com/ Utilities/RootkitRevealer.html]) can't fully get rid of the malware, you don't have to throw the drive away. That said, you will need to delete the drive's partitions, repartition the drive, and reformat its file system. Modern OSes let you do all of these things as you run their installation routines. Note that only a reformat and reinstall will get rid of some rootkits, as removal tools won't always work.

Use another PC with fully updated antivirus, antispyware, and firewall software to inspect all of your backup media for malware before you transfer any data back to your system. If any data is infected on a write-once backup medium, such as a CD-R, you might need to copy the files to another PC's hard drive, disinfect them, and then write them to a fresh CD-R. Of course, if you wait a few weeks before laundering your data this way, the security software on the second PC will be more likely to be immune to any malware on the backup media thanks to updates in the meantime.

Errors and data corruption. Some error messages have so many possible

Smart Computing's database of error messages (www.smartcomputing.com/techsupport/errorbrowse.as px) lists plenty of STOP errors, many of which indicate problems in the Windows OS (operating system).

causes that it's hard to categorically lay the blame for one on the OS. For instance, some STOP errors listed on a BSOD (blue screen of death) in Windows might be caused by any number of things, from bad RAM (random access memory) to data corruption to an OS fault. In general, BSODs are fairly serious, as are errors that multiply and keep you from being productive. Either case may warrant a reinstall.

Data can get corrupted on the hard drive by someone turning off the PC without shutting it down through Windows, as well as by a failing hard drive, a drive controller driver issue, or even a defragmenting session that went

awry. If Windows scans the hard drive for file system errors and bad sectors at every bootup, and you can't get it to automatically fix the errors in Windows Explorer (right-click C: or the relevant drive letter, then click Properties, Tools, and Check Now under Error-Checking), run a free diagnostic such as Seagate Seatools (www .seagate.com/support/seatools). If the hard drive turns out to be physically OK, a reformat (which maps out bad sectors) and reinstall should fix the trouble.

The Litmus Test

Basically, you should reinstall or repair your OS when you realize that it would cost you less time, effort, and money than trying to troubleshoot your system's problems piecemeal. For reference, installing WinXP from a CD may take less time that it will take to download the necessary Windows Updates afterward, especially if the CD doesn't contain Service Pack 2.

Factor in driver updates, application installs and setup, and data transfers from backup media, and you're talking about a couple of long afternoons. But if the result is a faster, trouble-free PC, that's time well spent. **RS**

BY MARTY SEMS

You Know It's Time To Reinstall When . . .

Any or all of the following may send you reaching for that OS installation CD, as long as you've first ruled out a hardware problem. For in-depth tips on things to try beforehand, flip forward to the "First Try This" section of this issue. It's time to reinstall when:

- Error messages are making it very hard to use your PC
- Your security software can't fully get rid of malware, such as spyware, a worm, or especially a rootkit
- System Restore doesn't solve the problem
- You can't find any useful advice online about your PC's error messages
- You can't keep applications from conflicting with each other, nor uninstall a troublesome app
- Updating relevant drivers, rolling them back to earlier versions, and/or cleaning out old drivers with a utility don't help