

Clean the hard drive before dumping your PC



By [Kim Komando](#)

If you're getting rid of your old computer, or even if you aren't just yet, there are some things you should know about it.

Chances are great there's sensitive data on it. If you're like me, that PC's hard drive contains a compilation of your personal and business life. If the wrong people were to grab it, they could hurt you and your business very seriously.

Here's the problem: An index of files is maintained for the hard drive, telling it where things are stored. When you install a file, especially a big one, it is scattered around the hard drive in bits and pieces. On your command to open the file, the hard drive checks the index, then gathers the pieces and reconstructs them.

When that file is deleted, the links between the index and the file disappear. That tells your system that the file is no longer needed and that hard drive space can be overwritten. But the deleted file remains on your computer. Only when it is overwritten do you begin to be safe. Even then, a specialist might be able to recover the old data.

Assuming you just deleted everything in preparation for saying goodbye to your PC, it is unlikely that the sensitive information has been overwritten. It's still sitting there, and anybody with a shareware program could find it.

Do you trust the recipient?

How you handle this really depends on where the computer is going. If a trusted employee or your Aunt Minnie is getting it, you can probably just delete stuff.

But be aware that if you're going to give the computer to a charity, you don't know where your machine will land. And if a neighborhood kid with a mean streak and too much time on his hands gets it, you could have real problems.

So here are my four suggestions.

1. Don't want a big hassle? Give the computer to a trusted employee, friend or family member. If you trust who you give it to, I wouldn't put a lot of effort into destroying data. Recovering deleted data isn't automatic. A thief or con artist will have to get some specialized software and learn to use it. Rivers of boring data would have to be sorted to find the good stuff. The average (honest) person isn't going to bother. So if you give the PC to someone you trust (careful now), you should simply delete the files. More extensive work probably isn't worth the effort. Just be sure the recipient is honest. If he or she is shaky, go to the next step.

2. Reformat the hard drive and re-install the operating system. Reformatting a disk prepares it to accept a new operating system. It also wipes out everything on the hard drive. That's your goal. Past versions of Windows (up through Windows Me) allow you to create a startup disk. You'll need one to reformat your hard drive. Click Start > Settings > Control Panel. Double-click Add/Remove Programs. Click Startup Disk. Click Create Disk. On Windows XP, you'll need to download the disk information. Go to [BootDisk.com](#) and click "DOS ? Windows 9X/NT4/2000/XP Excellent Bootdisks." Download the Windows XP Custom Install Disk and save it to a floppy. On all systems, shut down all open programs. Restart the computer with the floppy in the A: drive. At the A: prompt, type Format: C. Answer "yes" to the warning: you want to wipe out all the data. When the reformat finishes, put the Windows installation CD in the CD drive and remove the floppy. Restart and re-install Windows. Reformatting will keep most people out of your old files. But specialized shareware exists to reclaim files after reformatting. If you do not know who will get the computer ? or you do know and you don't trust them ? stronger measures are required.

3. Buy software and overwrite the disk, again and again and again. If you don't know much about computers, this might be easier than Step 2. There are several programs that write gibberish to the hard drive. They promise that nobody will be able to find your files after the software is utilized. PC Inspector's ([www.pcinspector.de](#)) e-maxx meets U.S. military standards. Another good program is DriveScrubber (\$29.95), from Iolo Technologies ([www.iolo.com](#)). If you have a Mac, try SuperScrubber ([www.jiiva.com](#)). It is \$30, and also meets military specs. This process can be slow, because these programs write to the disk repeatedly. You might want to run it overnight.

4. You're totally paranoid, so get out the acetylene torch. I'm not kidding. The only absolute and assured way of protecting your data is to destroy the hard drive. To do that, you need to remove it from the computer. If you want to save the rest of the computer, touch the machine's metal frame before reaching in. Static electricity can wreck the circuitry. The Pentagon shreds its hard drives. That should work, assuming you can find a hard-drive shredder. I've never seen one. You need to destroy the platters inside. Try smashing them with a hammer. Destroying them with a torch should work. Step 4 seems excessive to me. But you're right to be paranoid about this. Identity theft has become overwhelming. There are a lot of people out there who would love to hurt you. Personally, I would use Step 3. I believe in being careful, no matter who gets the computer.