

# Clean the Hard Drive Before Dumping Your PC

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.

## Is the Data Really Gone?

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. 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.

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 (through Windows ME) allow you to create a start-up disk. You'll need one to reformat your hard drive. Click Start > Settings > Control Panel. Double-click Add/Remove Programs. Click Start-up Disk. Click Create Disk. On Windows XP, you'll need to download the disk information. Go to [BootDisk.com](http://BootDisk.com) and click "DOS — Windows 9X/NT4/2000/XP Excellent Boot disks." 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.

If you don't know much about computers, this might be easier. 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. You can leave the operating system and other files on the hard disk, if you want. These programs can be set to overwrite only the unoccupied areas. The process can be slow, because they write to the disk repeatedly. You might want to run it overnight.

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. Unplug the wires on the hard drive and remove the mounting screws. The hard drive slides out from the back of its holder. The Pentagon shreds its hard drives. That should work, assuming you can find a hard-drive shredder (I use *Atlas Metals* in Denver). You need to destroy the platters inside. Try smashing them with a hammer. Destroying them with a torch should work. This seems excessive to me. But you're right to be paranoid about this. Identity theft has become overwhelming. Personally, I would use the overwrite process.

I believe in being careful, no matter who gets the computer.