

DESTROY YOUR DATA BEFORE YOU DUMP YOUR DRIVE

**Beginners' Kaffee Klatch
Presented by Bill Wilkinson
April 1, 2006**

You did it right, or so you thought. Before you gave your old computer to a friend or a charity, you deleted all of your email, all of your home finance files, all of your banking information, all your personal, private information.

If you think “deleted” information can’t be retrieved from an old hard drive, think again. Researchers have discovered that most computer users don’t bother to properly wipe their hard drives before getting rid of them. Deleting files just breaks the connection between the index portion of the hard drive and the file. The file itself does not go anywhere. To be destroyed, it has to be overwritten when a new file is saved.

Today, our hard drives contain information pertaining to almost every aspect of our lives, which makes them valuable tools for thieves looking for a quick buck. Even if you can’t see any remaining data on a hard drive, chances are there’s something still there, so it’s essential to learn how to erase it for good before you dump that drive.

Deleting files in Windows carries a certain sense of finality, which in turn leads many users to believe deleted files are gone forever. After all, when you empty the Recycle Bin, it seems you can never recover those files because Windows offers no option to get them back. However, the delete process does not actually erase files from your hard drive. Windows simply rewrites the data that points to the file, modifies a small amount of the file’s data to mark it for deletion, and then moves the rest of the file data to the hard drive’s free cluster list. Why does Windows simply move deleted files instead of erasing them for good? It’s easier for the operating system to move those clusters to your free list than to actually write zeros over them. So in order to make those deletes fast, that’s the standard way to do it.

Another popular misconception is that reformatting a hard drive will permanently rid the hard drive of all stored data. But like deleting files, formatting won’t do the trick. All the format command does is reconfigure your file allocation tables at the beginning of the disk and check through the disk to see whether the blocks are still readable. But it doesn’t do anything to remove or overwrite any of the data. Again, this is for performance reasons.

The file system's efficient behavior means that potentially all of the deleted data on your hard drive are vulnerable to recovery techniques, including the use of easily obtained software that can search a hard drive's sectors for deleted data and recover them. There are also several premium recovery services that claim high success rates when it comes to extracting hard drive data. Depending on who you are and what's on your hard drive, snoops can use even more aggressive and expensive techniques to scour your drive, including the use of a magnetic force microscope, which can even extract overwritten data.

Fortunately, securing your hard drive before you sell it, give it away, or throw it away is surprisingly easy. There are several methods you can use to ensure that all of the data on your drive—whether you previously deleted it or not—won't be recovered by anyone else looking to take advantage of your information.

For most users, overwriting data is the most efficient method for wiping hard drives. When all of the addressable blocks on a hard drive are filled with new data, typical recovery programs cannot retrieve the data that previously resided in the blocks. One way to overwrite is to fill your hard drive with large files and delete them, but a more efficient method is using any one of several software utilities specifically designed to overwrite hard drive data. These utilities offer a variety of wiping methods that deliver varying amounts of protection, and the method you choose should depend on the level of your data's sensitivity and the time you're willing to spend waiting for the wipe process to complete.

Even if you don't think your data is valuable, it's still worth the effort to wipe your drive before it leaves your hands. The pilfering of hard drive data is probably a common occurrence, especially considering that the process to extract the data is fairly straightforward and fairly easy. Even if you trust the person buying your PC or hard drive, you don't know where it will end up in the future, when it could hold your old data. You wouldn't sell your wallet with your license and credit cards still intact, so follow the same precautions with your hard drive.

When it comes to erasing hard drives, you won't find any wiping utilities included with Windows. But that's no problem because the choices available on the Web are vast and varied, and it's easy to find a program that suits your particular needs. Below are a couple FREE drive-wiping utilities that can help to secure your drive before you ditch it.

Darik's Boot And Nuke (DBAN) <http://dban.sourceforge.net>

If you want a free, no-nonsense tool that destroys all hard drive data, check out Darik's Boot And Nuke (also called DBAN). This nifty open-source utility lets you boot your computer with a floppy or CD and wipe your drive using any of several methods.

The CHAOS Shredder: If you want to be selective in the data you wish to erase from your hard drive, then you will want to consider this FREE product:

CHAOS Shredder allows you to purge, wipe and erase SELECTED (YOUR CHOICE) data with methods that far exceed US Department of Defense standards for file deletion (DOD 5220.22). <http://tinyurl.com/pdvye>