Make sure files you've deleted are truly gone

by Jonathan Sidener

Sooner or later, your computer is going to need an upgrade. You'll copy its vital files onto the new device and then recycle the now-obsolete hardware.

But what about those files? Did you delete them? Are they really gone? You had personal and credit information on there for friends, family and clients.

The answer far too often is no, the files aren't really gone. In the bad old days when everyone tossed their old technology in the trash, the dirt, moisture and bulldozers at the landfill provided a form of identity protection, but at a huge toxic price.

Now in California, recycling electronics is not only the right thing to do, it's the law. Recycling means consumers will have to take a few extra steps to protect their privacy and ensure that personal information doesn't end up lingering on hard drives shipped to crime-plagued places such as Nigeria.

To understand the complexity of the situation, think of your computer as a big, sophisticated bookstore. An inventory system tracks what's on the shelves as workers constantly rotate the stock.

When you delete a file, you're like the bookstore manager deciding to take a title off the shelves. But it doesn't disappear just because it's off the shelf.

In the book world, unsold titles have their covers torn off to be returned to the publisher for a refund. And traces of the books are removed from the inventory system.

In the computer world, something similar happens. The file has identifying information stripped off and the computer's inventory system no longer acknowledges the file.

In the publishing world, the coverless book is considered to have been returned to the publisher. The inventory system says it no longer exists. But in fact, it sits in a barrel or bin for some period of time. If you picked up one of these returns, you could read the whole book.

Deleted computer files are similar. The system will tell you that the files don't exist, but the data sit on the

hard drive - as complete as a book with its cover torn off - until the computer gets around to rewriting those areas.

It would be easy for whoever gets your computer to go back and restore those deleted files. If the computer is old and not reusable, you may want to destroy the hard drive - especially if the computer isn't working.

Unless you have passwords to a hefty Swiss bank account or national security secrets on the drive, a few sharp blows with a hammer or a little fun with a power drill should do the trick. Hard drives are impact-and dust-sensitive. A puncture wound or a flurry of hammer blows will keep them from telling your secrets to anyone.

Internet discussions on the topic point to many creative destruction techniques such as shooting the drives with high-powered rifles and melting them with welding torches.

If your computer still works and you'd like to see it put back to use, there's a more civilized option: file wiping. This process writes random characters over all the deleted files - overwriting data multiple times if you want - so the information is really erased.

There are several commercial file-wiping programs available, but experts caution that not all of them are 100 percent effective.

Modern operating systems on Windows, Mac and Linux computers often make hidden backup copies of files and programs. This is great when you have a problem and want to restore your computer to an earlier configuration. But it's a problem for effectively wiping old files.

The only sure-fire solution is to nuke, or totally wipe, the drive, deleting everything including the operating system. A popular free program, DBAN, or Darik's Boot and Nuke, is available from http://dban.sourceforge.net. The Web site has a support forum to help if you run into problems and detailed instructions, which may seem daunting to casual computer users.

Running DBAN entails three steps: Download the file. Run the file to create a boot disk on either floppy or CD. A boot disk is designed to run at startup, before the operating system launches. Start the computer from the boot disk, which launches DBAN.

Darik Horn, creator of DBAN, says just about anyone should be able to use the program. "The hardest part of

using DBAN is changing the computer boot order so that the computer starts DBAN from a floppy disk or a CD-R disk," Horn said. Some computers aren't configured to run a boot disk from the CD drive.

"If you can push Delete or F1 at the right time when the computer starts, and if you can find the boot menu afterward, then you can use DBAN," he said.

And there's no reason to worry about hurting an obsolete computer. If something goes horribly wrong with DBAN, just drag the computer into the backyard and get out the hammer. Search Google Images for hard-drive photos if you're not sure what to whack.

Make sure files you've deleted are truly gone by Jonathan Sidener