Hard drive cleansing: a guide for the paranoid

by Tom Gutnick, Sunny Banana IT Consulting

Are you getting rid of a computer? You probably want to remove any personal data first. There are several possible approaches, so consider the following questions:

- How paranoid are you? (I once had a boss who said, “Just because you're paranoid doesn’t mean they’re not out to get you.”)
- Given the paranoia, what is the likelihood that you are being specifically targeted by an organization (such as a domestic or foreign intelligence agency) with extensive resources? If high, they probably already have gotten what they need and aren’t waiting for you to dispose of the computer.
- How easily do you want to allow the old computer to be reused by somebody else?

Note the trade-off between security of your data and the ease of reusing the computer. I’ve listed a few approaches here, in decreasing order of security (and increasing order of easy reuse). Note also that I’ve not gone into great detail on many of these steps, since this is supposed to be a short document. If you can’t figure out the details, consider getting professional assistance. (I am talking about professional help from a computer geek, not a psychiatrist.)

Physical destruction of drive

1. Remove the hard drive from the computer. This is easy for most desktop and laptop computers, although newer laptops (especially from Apple) don’t provide an easily-accessible compartment. If you’re not sure how to get at it, Google is your friend. (Maybe Bing is your friend too?)
2. Smash the drive with a hammer. You do not need a sledge hammer — a regular hammer should be sufficient. Once the drive’s platter has broken into pieces, you’re good!

Notes:

- Put the drive inside a plastic bag before you smash it, and the pieces won’t go flying all over the place.
- Most municipalities prefer that electronic devices not be thrown in the regular trash, but rather are brought to recycling events. I assume this applies even if the device has been obliterated.

Logical destruction of drive

Download a free copy of Darik’s Boot and Nuke (DBAN), at `www.dban.org/download`. (Don’t do a Google search! Just go directly to the website I just gave you. Too many of my clients do a search, and end up clicking a link that has the software they’re looking for bundled with assorted crapware or malware. Use the official download site so you know you’re getting the right thing!)

The basic process is to create a bootable USB flash drive or CD/DVD. Boot from it to run the program. You’ll end up with a hard drive that has been completely wiped. All partitions on the drive are gone, including so-called “recovery” partitions which most PC vendors use these days instead of spending 50¢ to give you a CD or DVD with a backup copy of the operating system. You’ll need to install a fresh

copy of an operating system (Windows, Linux, etc.) before it can be used again

One little complication: newer PCs use UEFI (Unified Extensible Firmware Interface) instead of BIOS (Basic Input/Output System). Depending on how it was implemented on your computer, you might have to stand on your head to be able to boot from removable media instead of the hard drive. (It shouldn't a big deal, but it make take a little digging for the specific procedure.)

Logical destruction of files

This is perhaps the simplest method, and provides a reasonable measure of security. (This is the method I use the most often. Of course I have no way of knowing with certainty that no data has been compromised.) Although the details vary, the general method should work with any version of Windows, Linux, or MacOS.

1. Before you begin, download a free copy of Eraser Portable (`http://portableapps.com/apps/security/eraser-portable`) and install it on your computer. (This is a Windows utility. For Linux, use the built-in `shred` command, or install the `wipe` utility. For Mac OS X, use the Disk Utility; depending on your level of paranoia, you can use the *Zero Out Data* option or *7-Pass Erase* option.)
2. Also before you begin, make sure you know where all your data is located. The default location on Windows is C:\Documents and Settings\<*username*> or C:\Users\<*username*>, but make sure you know if any application program is writing to a non-default location. For Linux, look for /home/<*username*>.
3. Create a new user account, with administrative privilege. Log out from your other account and log in with this account.
4. Use your erasing utility to securely delete all the files from the default location and any other locations used. Note that most of these utilities allow you to specify the method(s) used to clear out the data. The trade-off is that the more security you want, the longer it will take.
5. Delete the old user account.
6. If you're really paranoid, you can defragment the drive partition — as the data gets shuffled around, it becomes harder still, even for an adversary with strong forensic abilities, to recover.

The advantage of this method is that your operating system is still intact, so it's easy to repurpose the computer.