



## 3 steps to take when disposing of your computer *Protect your credit -- and identity-- when trashing your hard drive*

*By Michael Berg*

September 7, 2010

Most people wouldn't throw out their Social Security card or toss a credit card in the trash. Yet careful souls worldwide have been dumping old computers by the millions, filling landfills with exactly that kind of sensitive information, where aggressive high-tech criminals can readily scoop it up.

According to the latest statistics from the EPA, 205 million computer products were disposed of in 2007, with a paltry 48 million of those recycled. That leaves plenty of identities in the garbage stream just waiting to be poached.

Indeed, many computers are being mined for Social Security numbers, credit card information, bank statements, investment records and various other tidbits that open the door for everything from credit card fraud to full-on identity theft. While exact numbers are difficult to come by, there's no doubt it's happening with ever more frequency.

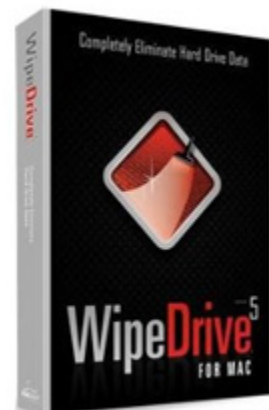
"I've personally met hundreds of people who have had their identity stolen this way," says John Sileo, identity protection expert and author of "Privacy Means Profit," available at [thinklikeaspy.com](http://thinklikeaspy.com). "The thing is, if thieves are smart -- which they are -- it should be a massive problem, because it's such an easy way to get data."

You don't have to be a victim. Taking these three simple steps when discarding a desktop or laptop computer virtually guarantees your private information can't be stolen.

### **Step 1: Permanently delete your data**

Cleaning off your computer is easy -- just move all files into the trash and empty it, right? Not exactly. "When you place a file in the computer's trash, it's simply marking it to be written over," Sileo explains. "That means until it's written over, the file remains on the hard drive. Unless you work with extremely large files on a regular basis, like video files, chances are you'll never write over all the old sectors throughout the life of your computer. 'Erasing' is a misnomer."

To be truly safe, you need to wipe the hard drive to Department of Defense standards, according to John Shegerian, co-founder, chairman and CEO of Electronic Recyclers International. To do this, you can buy a program such as [WipeDrive V5](#) (\$39.95 on Amazon.com), which comes in versions for Macs or PCs, or [Nova Drive Erase Pro](#) (\$29.95 on Amazon.com), which works with PCs only.



Or, save some cash by going the freeware route. "The program I like is Darik's Boot and Nuke (dban.org)," Sileo says. "It doesn't just erase or reformat your drive, which isn't good enough, it writes 1's and 0's over all of the old data." There are versions available for PCs and Macs.

### Step 2: Handle the hard drive

You have a few different options to keep your hard drive out of criminal hands. "You can take the hard drive out and save it in a safe," Sileo suggests. "If you're a business, that's not practical, but if you have, say, five computers over the course of 10 years, removing the hard drive is oftentimes less expensive and safer than destroying it in stupid ways."



Such "stupid" ways include soaking it in acid or water, waving a magnet over it, or taking a hammer to it. "None of that will effectively destroy the data," Sileo says. "Instead, buy one of those small screwdrivers to open hard drives and sand the platters. That's the most certain way of scrubbing the information -- all of the other ways are rubbish unless you have a professional company that uses an industrial-size shredder that grinds the

drive to nothing."

### Step 3: Discard responsibly

E-waste is the fastest growing solid-waste stream in the world, according to Shegerian. Because of that, options for proper disposal are much more accessible than they were even a few years ago. Best Buy and Staples, for instance, are two retailers that have a take-back program on electronics. There are also online options, such as Yourenew.com, where you can sell back old electronics, which will be wiped and resold or recycled; starting in September, Shegerian's company will offer a mail-in recycling service through electronicrecyclers.com. (To find all the options in your area, visit another of Shegerian's websites, 1800recycling.com.)



No matter which recycler you choose, the key consideration is certification.

"Make sure they're certified through the Basel Action Network e-Stewards program or Responsible Recycling (R2) certified," Shegerian says. "Then you know they have good practices and good downstream vendors where they're sending their commodities."

Take note: Even if you take out the hard drive and store it, you should still send the rest of the computer to a certified recycler. "There are hazardous metals in electronics like arsenic, lead, beryllium and cadmium," Shegerian says. "But if your laptop or desktop goes to the appropriate recycler, 99.8 percent of everything in there can be reused. It won't end up in a landfill." That means your data and your conscience are safe.

### Bonus step: Scramble your information

Even if you're not throwing your computer away anytime soon, there's something you can -- well, *should* -- do right now to protect your data. Whole-disk encryption will make it difficult for thieves if your computer is lost or stolen. "You can buy an encryption program like PGP (pgp.com), or there's freeware you can download at TrueCrypt.com," Sileo says. "Then if you lose the computer or it gets discarded in a way where it's not properly recycled, you already have one layer of protection."