When all else fails…

With Windows 7 and the advance of very cost-effective, powerful computers, many of you will be purchasing new computers in the near future. That raises the question of how to properly dispose of your old computer. You will either choose to give or donate your old computer to someone, or you will decide to discard it (hopefully by properly recycling it). In any case, you will want to make sure that all of your private data on the hard drive is properly deleted so that it cannot be extracted by others. In this day and age of identity theft, your hard drive is a prime target.

This is an article printed on April 3, 2003 in PC World. It is even more true today:

Hard Drives Exposed

We bought or salvaged ten used drives and found sensitive business and personal data on all but one.

Tom Spring, PCW Print
Apr 3, 2003 2:00 am

It's a chilly March Saturday at the Pit, a concrete holding pen for abandoned computer parts at the Needham, Massachusetts, town dump. Nearby, three locals wait patiently in their idling cars.

An SUV pulls up. Driver James Curtin grabs an old PC from the back and puts it into the Pit alongside other CRT monitors and old computer chassis. Slowly the other men exit their cars and walk toward the discarded computer--one with a screwdriver in hand.

For these PC scavengers, the Pit is a gold mine for memory chips, processors, and other components that they use to build PCs on the cheap. But they also routinely find something else: business and personal data that prior owners have left on discarded hard drives.

"[On] almost every hard drive I pull, I'll find a tax return or a resume," says David Burns, who describes himself as a Needham regular.

The lesson for PC users? Old hard drives don't always die--or fade away. Often they are salvaged and reused in other computers. And when that happens, the data and sometimes-grimy secrets of previous users go with them.

Properly sanitizing a hard drive before giving away or reselling a computer requires only a small investment of time and an inexpensive or free disk-erasing tool. But many people don't even do minimal cleanup.

Data Galore

An examination of ten used hard drives we bought or salvaged in the Boston area disclosed a wealth of sensitive data. On all but one of them, we found data, including confidential business, medical, and legal records; Social Security, credit card, and bank account numbers; e-mail; and even pornography.

Most of the information was easy pickings--even on four drives whose previous owners had attempted to erase data, either by deleting files and emptying the recycle bin or by reformatting the disk--measures that simply conceal the data from the operating system. Not surprisingly, the equipment's former owners were shocked to learn that strangers had accessed their information.

"I went through my PC and thought I had thoroughly deleted everything," Curtin said of his old TriGem 486.

A Boston computer store sold us a hard drive previously owned by an accountant--and crammed with four years' worth of his clients' payroll and tax information and employee Social Security numbers. The accountant said that his nephew, who worked at a computer store, had removed the drive while upgrading his old computer several months earlier. The accountant said that he never thought to ask his nephew what had become of the hard drive.

Similarly, a Salvation Army store in Cambridge, Massachusetts, sold us a PC that had once belonged to an attorney; it still contained bank account numbers, an active America Online account (and a stored password), and draft legal documents on its hard drive.

"I most certainly never expected my personal information would ever be more than just that--personal," said the attorney. He said his firm's IT consultant had promised to properly destroy the data.

Our samples confirmed the findings of a study conducted earlier this year at the Massachusetts Institute of Technology. Two graduate students, Simson Garfinkel (who is also a prolific technology writer) and Abhi Shelat, bought 158 hard drives on EBay and from online shops. Of 129 drives that worked, 69 had recoverable files and 49 contained personal information, including 3700 credit card numbers, medical data, and pornography. Only 12 of the usable drives had been properly purged.

"This is a serious problem," Shelat says. Businesses become vulnerable when they unwittingly share sensitive information. And individuals leave themselves open to identity theft, a potentially ruinous crime that the Federal Trade Commission received nearly 162,000 complaints about in 2002--almost double the 2001 total.

Resurrected Drives

Tossing your your old drive out with the trash is no guarantee that it--and your data--will find a quiet resting place in a landfill. And scavengers like those at the Needham Pit are only part of the picture. As more towns and cities ban PCs from their landfills, businesses are cashing in.

Computer Salvage of New England collects old PCs and cannibalizes them for parts that it then sells. Similarly, the city of Cambridge pays a recycling company called Onyx Environmental Services to haul off PCs left for curbside pickup. Onyx salvages the parts and resells them.

Research firm Gartner Dataquest reports that businesses and individuals took about 150,000 hard drives out of service in 2002. Meanwhile, reported incidents of data security compromised by improper disposal of unwanted PCs have increased exponentially, says Gartner research director Frances O'Brien.

"Companies don't think twice about giving hard drives a simple reformat and handing the PCs out to employees, charities, or whoever else can save them a buck on disposal costs," O'Brien says.

Deleted or Hidden?

Even when people reformat the hard drive, a motivated sleuth can retrieve data using tools such as Norton SystemWorks' Disk Editor or the free Disk Investigator.

We did this on a drive purchased at the Super Computer Sale (a traveling computer fair), and uncovered research, e-mail messages, and a log of Web sites visited by employees at Fairfax Financial Holdings of Ontario, Canada.

"It shouldn't have happened," said Brad Martin, Fairfax's vice president of investor relations. "We are going to make sure that something like this never happens again."

Another used hard disk we bought at the computer fair had no operating system. But we identified the previous owner--and extricated 20MB of data documenting activities unprintable in this magazine.

Being able to recover deleted data can be useful: Ask anyone who's ever accidentally trashed a file. Hard drive data can help nail criminals, says Tom Galligan, owner of Electronic Evidence Recovery of Tiverton, Rhode Island.

But honest PC users have a legitimate interest in destroying data when they discard an old PC. Curtin wishes he had been more careful with his old drive. "I'll never make that mistake twice," he says.

The problem is that when you erase a file on your computer, the actual data in the file is not overwritten. The space utilized by that file is simply marked as “free” for use by other data. Once other data is written in that space, the original data becomes unrecoverable. Even reformatting your hard drive isn’t good enough. The way to completely erase data is to write over the same physical spot on the hard disk multiple times with different patterns, thereby obliterating the original data. This is called

"disk wiping". There are a number of government standards that deal with this topic and include 18 secure wiping algorithms (the most frequently referenced is U.S. DoD 5200.28).

There are many available products that perform secure data erasure. Two recommended free products can be found on www.dban.org (for completely wiping an entire disk) and http://eraser.heidi.ie (for completely wiping Windows folders or files).

There is one other option for ensuring that a hard drive can never be written: remove the hard drive from your computer and obliterate it with a hammer. But if you choose this option, don't expect anyone to be able to reuse the hard drive again in the future ☺

As always, I hope you have found this information useful. If you do not wish to receive these emails in the future, let me know.

All the best!
Steve (650-222-4140)