SafeKids.Com

The Mercury News
The Newspaper of Silicon Valley

Hard drives dumped; information isn't

DON'T BE SMUG IN THINKING PERSONAL DATA HAS BEEN ERASED

By Larry Magid
Special to the Mercury News

(links to drive scrubbing software)

Whether you recycle your old computer, sell it, give it away or take it to the dump, you may also be giving away personal information, even if you think you erased everything on your hard drive.

Two MIT graduate students bought 158 used disk drives on the secondary market and found many ``had not been properly sanitized.'' They found personal information, even when the previous owner had attempted to erase the data or even reformat the entire drive. The pair, Simson Garfinkel and Abhi Shelat, found medical records, love letters, pornography and thousands of credit card numbers.

The researchers aren't the first to discover a treasure trove of personal information on used machines. In 2002, a journalist purchased a used computer at a thrift store that had once belonged to the U.S. Veterans Administration. The drive contained medical information including the names of patients with AIDS and mental health problems.

While some people make no effort to delete sensitive data, others are lulled into a false sense of security by using standard file deletion methods. Most are temporary at best.

The most common way to delete files in Windows and Macintosh is to drag the file into the Mac ``trash can'' or Windows ``recycling bin.'' While that removes it from the desktop it does not remove it from the computer. In fact, you can restore the file by simply opening the trash or recycling bin and dragging it back to the desktop.

Both the Mac and Windows allow you to go one step further by emptying the trash which appears to delete the file completely. The Mac, for example, asks you if you are sure ``you want to remove the item in the trash permanently.'' Windows asks if you're ``sure you want to delete all of the items in the recycling bin.''

But neither method is permanent. Erasing a file doesn't actually delete the data; it just removes the file name from the directory.

The data is still there. Deleting a file the standard way is a bit like crumpling up a piece of paper and throwing it in the trash can rather than running it through a shredder. The MS-DOS delete command doesn't have an obvious ``undo'' feature but it too can easily be reversed.

This can be good news if you've accidentally deleted something. But it's bad news if you want it permanently gone. Numerous software products are available that allow you to ``undelete'' such files. ``Undelete'' from Executive Software is one of many that will allow you to recover deleted files on Windows. There are versions of VirtualLab data recovery software for both Windows and Macintosh. You can even try it out for free.

At first glance, formatting a hard disk sure seems like a pretty good way to obliterate your data, but it's not. The Windows Format command will warn you that ``Formatting will erase ALL data on this disk,'' but, again, that's not entirely true. While it will make the disk appear to be empty, that data itself will not be erased. The same is true with the fdisk command which creates and deletes hard drive partitions. There are numerous programs that can bring back seemingly eradicated from formatted hard drives. ``Recover it All'' from DTI Data advertises that it can ``Recover data lost due to Format, Fdisk, virus attack, deletion and many other scenarios.''

Someone looking to gather your personal information from a discarded disk drive doesn't even need any particularly expensive or exotic software. The popular Norton System Works ($69) includes Norton UnFormat and Norton UnErase that can often do the trick. But you don't even have to spend anything to get your hands on such software. If you visit the File & Disk Management section of Download.com, you'll find numerous ``free to try'' programs designed to recover deleted files or formatted disks.

In addition to the files that you know about, your hard disk may contain personal information in ``temporary'' files such as a browser or print spooler cache. These files are created automatically but they are not necessarily deleted automatically. Another source of ``hidden'' personal information includes e-mail programs which sometimes archive your incoming and outgoing messages.

Of course, anything sent via the Internet might also be stored on a server, a remote backup system or someone else's computer. During the Iran Contra scandal, it was revealed Oliver North thought he had destroyed thousands of e-mail messages only to find out they had been archived from the e-mail system's backup tapes.

Software Can Scrub Drive Clean

Fortunately, there are many programs -- including some that are free -- that can protect your privacy by ``sanitizing'' your hard drive. The most common method involves ``overwriting'' a file or an entire disk by replacing the old data with new ``null'' data such as zeros. With the exception of top secret documents, the U.S.

Department of Defense's ``clearing and sanitizing standard'' recommends that defense contractors ``overwrite all addressable locations with a character, its complement, then a random character and verify.''

Another option -- which most of us will probably never use is to ``disintegrate, incinerate, pulverize, shred or melt.''

Unless you're engaged in international espionage, sanitizing a drive by overwriting the data is probably adequate protection but it is theoretically possible for someone with the resources of the National Security Agency to recover the data using very sophisticated methods and equipment.

Still, Garfinkel and Shelat refer to these extraordinary methods as ``exotic'' and conclude that ``simply overwriting user data with one or two passes of random data is probably sufficient.''

There are also a number of free and shareware file erasure programs that you can obtain from Download.com and other file downloading sites. ``Sure Delete,'' from Wizard Industries (**www.wizard-industries.com**) is a free program that uses a wizard interface to give you a ``clean, secure, evidence-free hard drive in a matter of minutes.''

Macintosh OS X users can download a free copy of SafeShred from CodeTek Studios (www.codetek.com/) which claims to provide ``a virtual file shredder'' that completely shreds the file. For $15 you can buy ShredIt from Mireth Technologies (**www.mireth.com**) for

Macintosh OS 8/9 as well as OS X.

With these tools you can dispose of your PC and keep your secrets. Remember, you have the right to remain silent. And so does your discarded hard drive.

Drive Scrubbers

Autoclave - Secure Disk Deletion Free

Erase Delete Erasure Wipe & Overwrite by CyberScrub $39.95

Data Scrubber from Data Devices International $1695

PowerQuest Corporation - Proven Solutions for Storage Management $90

Acronis Privacy Expert Suite ($39)

Eraser Free

DataEraser™ Software - $30 to $500

AccessData - WipeDrive $39.95

UniShred Pro - Secure Disk Overwriting $450

Wipe Secure File Deletion (Linux) Free

Wiperaser XP $24.95

Source: Simson Garfinkel and Abhi Shelat

HOME ARCHIVES KIDS BOOKS LARRY'S BIO APPEARANCES EMAIL LARRY

SafeKids.Com