



What should you do with old computers and hard drives?

Thinking about purchasing a new computer, or do you already have a few older computers in your garage? Before throwing away those old computers you should consider what information is still on them, you may be giving an identity thief a goldmine.

If you are planning on getting rid of any computer that has been used to store personal information on it, think twice about who you give it to. Simply deleting your personal files or even reformatting the hard drive does nothing to permanently get rid of files once stored on a hard drive. Often people hand down older computers to family or friends, or sometimes donate it to an organization. While you may feel comfortable with the people you give your used computer to now, what about when they hand it down or throw it away?

A few years ago I assisted a group of Southern Oregon University students with a capstone project to see just how much personal data is available on older computers. The students would purchase old computers at yard sales and thrift stores and then examine the contents of the hard drives. It was absolutely amazing what information was recoverable with little computer knowledge and some free software available on the Internet.

A highly publicized example of this was demonstrated in 2006 when MSNBC ran an article about a 77 year old man named Hank Gerbus from Ohio. Mr. Gerbus purchased a new computer from Best Buy and several months after the purchase he returned the computer due to some hard drive failures. Best Buy replaced his hard drive with a new one and assured Mr. Gerbus that his old hard drive would be destroyed. Mr. Gerbus, worried about the information on the old hard drive asked to have it back, however Best Buy refused and said it would be taken care of.

A few months later Mr. Gerbus received a disturbing phone call at his home from a man in Chicago. The man told Mr. Gerbus that he had just purchased his hard drive from a flea market for \$25.00 and when browsing the hard drive found information about Mr. Gerbus' bank accounts, retirement information, and personal information about his entire family.¹ Luckily for Mr. Gerbus the person who bought his hard drive was not an identity thief.

Another study was done in 2002-2003 by MIT about used hard drives sold by retail outlets. Of 129 hard drives purchased, only 12 were properly cleared of data by the resellers. In fact one hard drive purchased by the MIT researchers contained 3,722 credit card numbers on it. They also found one that had been in an ATM machine and contained sensitive bank data.²

There are several options available if you are planning on getting rid of a computer. These include:

- Removing the hard drive and storing it in a safe place within your home and getting rid of the rest of the computer
- Removing the hard drive and having it shredded by a professional company (there are several in the Rogue Valley)
- Having the entire computer (hard drive included) shredded and properly disposed of
- Donating the computer minus the hard drive to a family member, friend, or organization. The recipient can pick up a new hard drive without paying too much money
- Physically destroying the hard drive yourself. Drilling a few holes through the middle of the hard drive is a very effective way of ensuring data won't be extracted

There is software available that can ensure the data on a hard drive is removed permanently, but unless you are quite computer savvy I would not rely solely on this alternative. If the software is not setup just right, there still may be recoverable data on the hard drive.

For anyone who does online banking, electronic tax preparation or other sensitive work on a computer, these steps should always be taken. If you are unsure about how to remove a hard drive there are many resources on the Internet and many computer repair business in the valley that can do it for you in a matter of minutes.

References

¹ http://redtape.msnbc.com/2006/06/one_year_ago_ha.html

² http://www.computer.org/portal/cms_docs_security/security/v1n1/garfinkel.pdf

Written by Sergeant Josh Moulin

Southern Oregon High-Tech Crimes Task Force