Blog for MPA Networks

https://www.mpa.com/blog.aspx?p=data-sanitization-erasing-old-pcs-completely

Data Sanitization: Are You Erasing Your Old PCs COMPLETELY?

Posted June 7, 2016

One of our pet peeves with some of our new customers is that once we come in to upgrade their IT network, they're careless about disposing their old hardware—specifically, their PC hard drives. They think that by simply deleting their existing files—email, customer records, and other sensitive or proprietary data—that information will be fully erased and irretrievable. That couldn't be further from the truth.

Deleting a file merely tells the computer that the space it occupies on the hard drive is no longer deemed "protected." **It will physically remain on the drive—encoded in ones and zeros—until those binary digits are *overwritten* by new data.**

If your desktop or laptop PC has reached the proverbial "end of the line," there won't be any further input to write over those old files. Before it leaves your control forever, you'll need to take additional steps to ensure its hard memory is absolutely wiped away.

How Clean Is "Clean"?

For many years, the gold standard for data sanitization was the Gutmann method, where the entire drive was manually rewritten—all in ones or zeros, or binary gibberish—a whopping 35 times, or *passes.* Today there are a range of standards employed around the world. **Our Department of Defense (DoD) considers three passes to be sufficient for national security.**

Data wiping isn't as complicated as it might sound, though there are a few differences between the traditional rotating hard disk drives (HDDs) and the smaller, flash-based solid state drives (SSDs) commonly built into laptops. It can actually be a DIY project, thanks to several time-tested freeware utilities favored by IT pros and computer geeks alike:

- Eraser thoroughly overwrites all or selected files of an HDD drive—from the Gutmann 35-pass standard downward. It can also be configured to wipe specific files or sectors of the drive on a regular basis.

- Roadkil's Disk Wipe effectively cleanses data from both internal HDD and SSD drives, via multiple passes (we recommend at least the DoD standard of three).

- Darik's Boot and Nuke, commonly known as DBAN, has remained largely unchanged since the earliest versions of Windows (forgive the primitive interface's resemblance to the infamous "Blue Screen of Death"). While DBAN still holds an excellent reputation as a comprehensive HDD data cleanser, like most utility software of its era, it can take a full day or more to finish the job.

"Non-Technical" Alternatives

It's also possible to render a hard drive permanently inoperable using simple methods: a hammer, power drill, or hacksaw—anything to physically destroy it. Some electronics recyclers around the Bay Area will feed your hard drive into a shredder, for an additional fee. **Whether you rely on software or brute force, *never* say goodbye to a computer before knowing its hard drive can *never* be accessed again.**

For more ideas about the full "life cycle" of IT data security, talk to us.