Spring Cleaning

Be Green, Not Blue

CYBER SECURITY APRIL 2018

As you upgrade your personal devices to the newest options, do you recycle the old equipment? Being green shouldn't make you blue. Take steps now to remove anxiety later that forgotten sensitive files on your last laptop could become a source of embarrassment or identity theft. Trying to securely delete data at the time you decommission equipment can turn into a multihour chore and a source of stress, but it doesn't need to be that way.

Make sure saved copies of your tax filings, personal photos, and other sensitive files can't be retrieved by the next person with access to your computer's drive by making the drive unreadable to anyone else. Dragging files to the trash or recycle bin doesn't remove data—it just removes the retrieval path to the file and marks that storage space available for other data to occupy sometime in the future. Your pirate treasure is still buried, but the map is missing. "Secure file deletion" functions go a step further to overwrite the data in those locations with random bits immediately.

The introduction and growth of solid state drives in consumer electronics, however, makes overwriting the data in these spaces less dependable than in the standard hard drives of the past. Today's "delete/overwrite" protection comes most reliably from full disk encryption (aka whole disk encryption), which encrypts all data on the machine—including the operating system and temporary files you weren't even aware you created. Follow the motto of a famous infomercial to "set it [full disk encryption] and forget it [the password/key]!" Even if someone removes the drive and puts it into a different machine, the encryption remains in place.

Plan A

Encrypt the full disk now using built-in functionality. Create a strong passphrase or password, since this becomes the decryption key! Everything will be encrypted, including the operating system, so you will have to "unlock" the encrypted drive with your personal passphrase every time you start or boot up your computer. Save the generated recovery key somewhere secure (like a password manager or printout stored in a secure office), in case you forget your password and need to access the data on that machine. Here are instructions for some of the most common built-in encryption functions:

- FileVault 2 (Mac OS)
- BitLocker (Windows 10 and Windows 8 Professional)
- BitLocker (Windows 7 Ultimate)

Plan B

If full disk encryption wasn't a built-in option, find a free or fee version of full disk encryption software that works with your operating system and personal capability. Check your favorite review sites or try Slant for recommendations.

Failsafe

Hammer time! Remove and destroy the drive (Geek Squad offers a three-minute tutorial on hard drive disposal). Most retail stores that accept computer donations for safe recycling will remove the drive and give it to you for secure destruction—just ask them to do that. Smash it, drill it, or hold onto the drive until there's a secure shredding event at work or in your community.