The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Securely wiping your hard drive
- How to recycle your computer

This month we discuss how to safely dispose of your computer. You may not realize that when you delete private information from your hard drive, the sensitive data is actually still there.

Securely Disposing of Computers and Other Storage Devices

GUEST EDITOR

The Ouch! team would like to welcome and thank Mr. Rob Lee as our guest editor. Mr. Lee is head of SANS' forensics program and maintains the SANS forensics blog at http://computer-forensics.sans.org.

THE PROBLEM

Eventually, every computer system gets replaced. Regardless of whether you discard, recycle, repurpose, donate, or sell your old computer, take steps to ensure that sensitive information stored on your system has been permanently obliterated – an essential security measure known as "sanitizing" the media. News stories about confidential information and trade secrets being snatched up from secondhand computers are common and troubling. That's because completely deleting or destroying the information stored on your hard drive is more complicated than you would think, and recovery of that data by a third party can be easier than you would expect.

Over the course of its life just about every computer system, whether it was used for business and/or personal use, has probably contained information that could be considered personal or confidential. Identity thieves and other criminals love to get their hands on that data and can often find it easily by examining used computers, disk drives, USB sticks, mobile phones, memory cards, etc., readily found in the trash or purchased in the open marketplace for pennies on the dollar.

Just because you didn't intend to save personal data on your hard drive does not mean there is none on it. Simply browsing the web can result in your hard drive storing data that can be pieced together to reveal a great deal of information about you.

WHAT DOES NOT WORK AND WHY

• Deleting Files

Simply deleting a file, in most operating systems, is analogous to entering a library and removing a book's index card from the card catalog. If you search the catalog *(your disk directory)*, the book *(your file)* appears not to be there because you no longer see its name. However, if you wander around in the stacks *(perform a low-level search of your disk),* you'll probably find the book *(your file)* intact, sitting right where it should be on the shelf *(your disk)*. And, your file will usually remain intact until another one just happens to overwrite the portion of your disk occupied by

Securely Disposing of Computers and Other Storage Devices

your first file. If you have a large disk with a lot of empty space, overwriting might not happen for a very long time or at all.

• Reformatting Your Disk or Deleting Disk Partitions

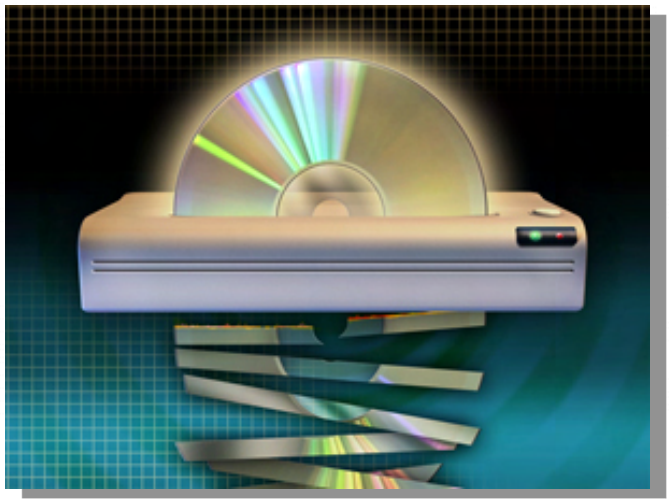
Both are only slightly better than deleting files, and both are still far from secure. Using the library analogy, these strategies are comparable to destroying the card catalog and removing the books from the shelves, tearing out the pages, and scattering them on the floor. The information in the books – what's left of them – is still there and can be recovered in whole or in part. Even if you install a new operating system on top of your old one, you can still recover many of your previous system's files.

• Encrypting Disks or Files

Encryption is an excellent anti-theft measure and legally required for certain types of data, such as patient or cardholder information. If your device is lost or stolen, disk or file encryption is often your last line of defense against the bad guys. However, because your information is only hidden from view, this protection is only as strong as your password and encryption method. A weak password will expose your data to risk regardless of how your information has been encrypted, and almost all encryption schemes can be cracked with sufficient time and effort.

WHAT DOES WORK AND WHY

There are really only two ways to obliterate your data permanently. *(National Institute of Standards and Technology – http://bit.ly/3vxB1)*



• Physically Destroying the Device

You can use heat, a strong magnetic field, shredding, pulverizing, and other violent methods that may require special tools and/or safety precautions. Many office document shredders are powerful enough to chew up CDs, DVDs, and floppies, which is a perfectly good way to dispose of your removable media and their contents securely. However, your hard disk drive might turn out to be much tougher to flatten or break than you'd expect.

• Securely Wiping Magnetic Drives

This is an effective method of sanitizing a re-writable storage device (such as a disk drive). You use a special software tool to overwrite every bit and byte on your disk so your original information cannot be read or recovered. There are several issues to consider as you prepare to wipe your computer's hard drive or other storage devices.

Back up data you want to keep.

Once you start the wiping process, there is no turning back.

Securely Disposing of Computers and Other Storage Devices

Use a specific program.

Secure wiping requires a special-purpose program, often found on a bootable CD or available via download. Refer to the list on the right. The program may present a question or two on-screen about how rigorous you want the process to be, as well as a point-of-no-return warning ("Are you REALLY sure?").

Set aside sufficient time.

Expect a secure wipe to take at least several hours, particularly on older systems and large hard drives.

Consider rules and regulations.

Although it used to be necessary to overwrite a disk multiple times with varying random patterns to ensure complete data obliteration, one time is sufficient to wipe your information. That said, industries that deal with confidential information routinely, such as health care, finance, defense, etc., should consider state and/or federal laws, industry guidelines, and company policies that precisely dictate how devices must be sanitized.

(National Institute of Standards and Technology – http://bit.ly/3vxB1)

Inspect before disposing.

Regardless of which method and process you select, inspect your sanitized media afterward to ensure that all information has been made unreadable.

Have questions?

Consult IT at the office or your computer support provider.

FREE WIPING TOOLS

Advanced Method:

ATA Secure Erase (Linux/DOS) – http://bit.ly/bZ1P2q

Alternative Methods:

DBAN (any operating system) – http://bit.ly/J2w4
SDelete (Windows) – http://bit.ly/RNzH6
Disk Utility (OS X) – http://bit.ly/aZeUzn
Linux – Use the built-in *dd*, *wipe*, and *shred* tools.

WHERE TO RECYCLE

After sanitizing your old computer, consider donating it to a charitable organization that may be able to give it a new life. The links below will help you donate, recycle, or discard your equipment in an environmentally-responsible manner.

TechSoup Stock – http://bit.ly/d8Hdht
ecosquid – http://bit.ly/96Vgb8
e-Stewards – http://bit.ly/8YEwvf

LEARN MORE

To subscribe to the monthly Ouch! security awareness newsletter, to access the Ouch! archives, or to learn more about SANS security awareness solutions, please visit us at http://www.securingthehuman.org.

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Alicia Beard, Carmen Ruyle Hardy