How to Clear Your Data off a Device

Before you ditch a device, you need to make sure none of your data is retrievable. Here's how to do it.

By Preston Gralla Aug 8, 2012 5:48 AM

If you're recycling your computer, smartphone or tablet, there's one significant problem you may have ignored: If you don't wipe them clear of data, you could become a victim of identity theft. Merely deleting files using normal system tools won't really do the trick --- you need to do a much deeper cleaning. Here's how to do it.

(Note: This article is an update of a previous article that ran in December, 2007; while some of the older information still stands, a lot of other things have changed since then.) **(**See Related: Hard Drives Exposed**)**

Cleaning up cell phones, smartphones and tablets

Smartphones and tablets essentially pack your entire life into a small package, including your contacts, emails, records of incoming and outgoing phone numbers, social media information...and more. So you want to make sure that someone else can't get access to all that information.

You could try deleting individual apps and contacts, but the odds of doing that effectively are close to zero. Instead, you want to do a complete reset of your phone to wipe out its data and restore it to its factory settings.

How you do this varies from operating system to operating system, and sometimes even device to device. These are general instructions that should work with most devices; however, it's best to check with your manual or manufacturer just to make sure.

Android: For versions before Android 4.0, press the Menu key from the Home screen and select Settings/Privacy/Factory data reset. You'll get a warning screen. Scroll toward the bottom and tap "Reset phone." If you also have an SD card in the phone (and don't want to use the data in your next phone), also make sure to check the box next to "Erase SD card."

Image Credit: iFixIt

ook for "Backup and reset." Tap that, and then, on the next screen, tap "Factory data reset." You'll get a warning screen along with a list of all the accounts you are currently signed into.

tap "Erase all Content and Settings." (This is specifically for Version 5; the process may differ slightly for other versions.)

then tap the Application Menu Key and select Settings/ System/About/ and tap the "Reset your phone" button.

BlackBerry: Head to Options/Security options/General settings, and then tap menu. Then select Wipe Handheld.

Wiping computer hard drives

Deleting files, folders and applications -- and clearing the data from the Recycle Bin -- won't do the trick if you're going to recycle your computer. Anyone can easily recreate that data using commonly available tools. Even if you reformat your hard disk, if someone really puts their mind to it they can recreate the deleted data.

This can be a serious problem. Back in 2003, two graduate students at MIT's Laboratory for Computer Science bought 158 used hard disks from eBay and other sources.

Only 12 of the drives had their data properly cleaned. Even though approximately 60% of the hard drives had been reformatted and about 45% had no files on them (the drives couldn't even be mounted on a computer), the students were still able to recover data from them, using a variety of special tools. They found over 5,000 credit card numbers, personal and corporate financial records, medical records and personal e-mails.

What can you do to keep your data safe? Get a disk-wiping program, preferably one that meets the U.S. Department of Defense's Media Sanitation Guidelines. These programs will overwrite your entire hard disk with data multiple times, ensuring that the original data can't be retrieved. If you use them, be patient, because it can take several hours to wipe the hard disk.

One well-known free application that meets the DoD's standards, according to Auburn University, is Darik's Boot and Nuke. The software creates a boot disk that wipes everything on the hard drive. It can also be used with floppy disks (remember those?), USB flash drives, CDs and DVDs.

Another free Windows utility that also meets the DoD's standards is Eraser.

If you've got a Mac, you can use Apple's built-in Disk Utility (it can be found in the Applications/Utility folder). You can also download a third-party application like Mireth Technology's ShredIt X ($25, free trial available), which lets you shred files (in other words, overwrite the contents of a file multiple times) as well as wipe your local hard drive, network hard drives and CD-RWs. (There's a Windows version as well.)

If you're truly nervous, there are hardware devices available that let you sanitize your drives such as Drive eRazer Ultra. Or you can pull the disk from your PC and send it to a hard drive shredding service that will physically destroy the drive.

(For a more tongue-in-cheek view of how to cleanse a hard drive, check out this old-but-still-good story: Removing hard drive data -- the YouTube way.)

Once you've wiped your device clean, it's safe to sell, donate or recycle your equipment. Find out how to do it in our article How to recycle your phone, PC and other tech gear.

Preston Gralla is a contributing editor for Computerworld.com and the author of more than 35 books, including How the Internet Works (Que, 2006).

See more by Preston Gralla on Computerworld.com.

Read more about data storage in Computerworld's Data Storage Topic Center.