US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Disposing of Devices Safely

Linda Pesante, Christopher King, and George Silowash

The Need to Protect Your Information

Getting a new computer, notebook, tablet, or other technology can be both necessary and enjoyable. Afterward you may decide to dispose of your old equipment. Whether you have your device recycled, give it to a friend, or donate it to a charity, a school, or a soldier, you need to protect the information on it from exposure. However, removing your information is harder than it seems. Systems are set up to protect us from losing information we need—when we delete a file, we can still get it back. Similarly, others who get your discarded computer or other device can get it back, too.

You need to take extra steps to remove information from your computing devices before you discard them. Otherwise, you risk exposing your private information, such as insurance and banking information and account numbers; tax information and social security numbers; health information; and passwords. You face the risk of identity theft. If you have computing devices for your business, you risk exposing sensitive information, such as customer names, addresses, and accounts; and employee payroll and benefit information. At risk are your business reputation, customer confidence, liability for exposing health information, and financial losses.

Removing information from computing devices is called *clearing.* The National Institute for Standards and Technology (NIST) states that clearing is "a level of media sanitation that does not allow information to be retrieved by data, disk, or file recovery utilities. It must be resistant to keystroke recovery attempts from standard input devices [such as a keyboard or mouse] and from data scavenging tools."

In this paper, we will discuss good practices for clearing information from computer drives, USB "thumb drives," and CDs and DVDs. We will also include advice regarding phones and tablets.

Techniques for Removing Information

Three ways of removing information from your computing devices, from the least effective to most effective, are deleting, overwriting, and physically destroying the device holding your information.

Deleting

Deleting information is not effective. It removes pointers to information on your computer, but it does not remove the information. Do not rely on the deletion method you routinely use when working on your computer—moving a file to the trash or a recycle bin, or choosing "delete" from a menu. Even if you "empty" the trash, the information is still there. It can be retrieved.

Overwriting

Overwriting is effective on all computing devices. It puts random data in place of your information, which cannot be retrieved because it has been obliterated. While experts agree on the use of random data, they disagree on how many times you should overwrite to be safe. While some say that one time is enough, others recommend at least three times, followed by "zeroing" the drive (writing all zeroes).

A number of overwriting tools are available, some of which are open source and freely available. For your convenience, here are some examples of open source tools. US-CERT does not endorse or support these products.

> Darik's Boot and Nuke (DBAN) (http://www.dban.org/) is a popular tool that completely wipes the drive. Eraser (http://eraser.heidi.ie/) can be used to securely remove individual files as well as all files. Avoid using these tools, though, if you have a solid-state drive.
>
> Secure Erase (http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml) and Parted Magic (http://partedmagic.com/doku.php) can be used on all types of drives, as long as you select "secure delete." Parted Magic provides many tools along with its data sanitizing tools.

You can find more open source tools and commercial tools on Wikipedia (https://en.wikipedia.org/wiki/List_of_data_erasing_software) and by searching the web.

Physical destruction

Physical destruction is the ultimate way to prevent others from retrieving your information. Of course, you should physically destroy the device only if you do not plan to give it to someone else.

Specialized services will disintegrate burn, melt, or pulverize your computer drive and other devices. If for some reason you do not wish to use a service, it is possible for you to destroy your hard drive by drilling nails or holes into the device yourself or even smashing it with a hammer. Fisher's article, listed in "Further Reading," contains more details. Fisher also warns to never burn a hard drive, put it in the microwave, or pour acid on it.

Some shredders are equipped to destroy flexible devices such as CDs and DVDs. If you smash or shred your device yourself, the pieces must be small enough that your information cannot be reconstructed; 1/125" is ideal.

Magnetic devices, such tapes, hard drives, and floppy diskettes, can be destroyed by degaussing—exposing them to a very strong magnet. Degaussers can be rented or purchased. Because of the expense, degaussing is more appropriate for businesses than individuals. It should

not be used if someone else will be using the device because degaussing destroys not only the information but also the "firmware" that makes the device run.

Advice About Mobile Phones and Tablets

Although the exact steps for clearing all information from your mobile phone and tablet is different for each brand and model, the general process is the same.

1. Remove the memory card, if your device has one.
2. Remove the SIM (Subscriber Identity Module) card.
3. Under Settings, select Master Reset, Wipe Memory, Erase All Content and Settings, or a similarly worded option. You might need to enter a password you have set, or contact a local store that sells the equipment for assistance with a factory-set password.
4. Physically destroy the memory card and SIM card, or store them in a safe place. (Memory cards can typically be reused, and SIM cards can be reused in a phone that has the same carrier.)
5. Ensure that your account has been terminated and/or switched to your new device.

For detailed information about your particular device, you can consult online documentation or the staff at your local store.

Conclusion

Computing devices allow us to keep a great deal of information at our fingertips. When we dispose of a device or pass it to someone else, we risk exposing information to people who should not have it—an improperly disposed of device can contain a wealth of useful information. You can protect the information you have stored electronically by following the recommended practices in this paper.

Further Reading

Bradley, Tony. "Prepare Your Hard Drive for Disposal," *former About.com Guide.* *netsecurity.about.com/od/quicktips/qt/erase_drive.htm*

Fisher, Tim. "How To Completely Erase a Hard Drive," *About.com Guide.* http://pcsupport.about.com/od/toolsofthetrade/tp/erase-hard-drive.htm

Garfinkel, S. L. "Remembrance of Data Passed: A Study of Disk Sanitization Practices," *IEEE Security and Privacy* 1, 1: 17-27. ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1176992&tag=1 (2003).

Henry, Alan. "How Do I Securely Wipe a Computer?" *LifeHacker.* http://lifehacker.com/5835369/how-do-i-securely-wipe-a-computer-before-donating-it-to-charity

Hughes, Gorden F.; Coughlin, Tom; & Commins, Daniel M. “Disposal of Disk and Tape Data by Secure Sanitation,” *IEEE Security and Privacy 7*, 4: 29-34. ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5189559&isnumber=5189548&tag=1 (2009).

McDowell, Mindi & Lytle, Matt. “Effectively Erasing Files” (US-CERT Cyber Security Tip ST05-011). http://www.us-cert.gov/cas/tips/ST05-011.html (2010).

NIST: Kissel, Richard; Scholl, Matthew; & Li, Xing. *Guidelines for Media Sanitation: Recommendations of the National Institute of Standards and Technology* (NIST Special Publication 800-88). http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf (2006).

wikiHow. “How to Delete Cell Phone Memory. http://www.wikihow.com/Delete-Cell-Phone-Memory (last updated June 2012).