# How to delete information securely

Most of us think that a file on our computer is deleted once we put the file in our computer's trash folder and empty the trash; in reality, this does not actually delete files ? it just makes them invisible to the user until the space they took up on your computer is overwritten with something else. This means that, with the right tools, your ?deleted? files can often be retrieved.

The best way to delete a file forever, then, is to make sure it gets overwritten immediately.  
This can be done easily using Eraser (for Windows) or Secure Delete (for Mac OS X), both of which are described below. Users of Linux and other open-source operating systems can use GNU shred, but this requires a more advanced technical proficiency.

Note that securely deleting data from solid state drives (SSDs), USB flash drives, and SD cards is very hard! The instructions below apply only to traditional disk drives. If you?re using an SSD or a USB flash drive, you can skip to the section about it below.

# Secure deletion on Windows

On Windows, we suggest using Eraser. Eraser is a free/open source secure deletion tool for Windows, and is much better than the built-in tools. To use Eraser, first [download the installer](eraser.heidi.ie/download.php) from its website; make sure to choose a ?stable? build. After the file downloads, double-click on it to launch it and Run the file.

Once Eraser is installed, if you want to securely delete a single file or folder, simply:

* Right-click on the file or folder and choose Eraser > Erase from the right-click menu.

Alternatively, you may want to securely erase all the previously deleted data from your computer.

* Launch Eraser.
* Click the downward-pointing arrow next to ?Erase Schedule? and choose ?New Task.?
* In the ?Task Properties? dialog that pops up, set the ?Task Type? to ?Run immediately.?
* Then click the ?Add Data? button near the bottom of the dialog.
* In the new ?Select Data to Erase? dialog that pops up, choose ?Unused disk space? and make sure the correct disk drive is selected in the drop down box (most likely the ?(C:)? drive).
* Click ?OK? to exit both dialogs, and Eraser should start erasing.
* Once it?s done erasing, the task will disappear from the list of tasks in the ?Erase Schedule.?

# Secure deletion on Mac OS X

On OS X 10.4 and above, you can securely delete individual files by simply:

* Moving them to the Trash;
* Then selecting Finder > Secure Empty Trash.

Alternatively, you may want to securely erase all the previously deleted data from your computer. Apple's advice on this is to:

* Open Disk Utility (in Applications/Utilities);
* Choose Help > Disk Utility Help;
* Search for help on erasing free disk space.

# Limitations

Unfortunately, there are limitations to secure deletion tools. Even if you follow the advice above and you?ve deleted all copies of a file, certain traces of deleted files, such as its name will probably continue to exist for some time on your computer. Overwriting the entire disk and installing a fresh operating system is the only way to be 100% certain that records of a file have been erased.

You may be wondering, "Could I search the raw data on the disk to see if there are any copies of the data anywhere?" The answer is yes and no. Searching the disk will tell you if the data is present in plaintext, but it won't tell you if some program has compressed or otherwise coded references to it. Also be careful that the search itself does not leave a record!

# Computers and hard-drives

If you want to finally throw a piece of hardware away or sell it on eBay, you'll want to make sure no one can retrieve your data from it. And even if you're not getting rid of it right away, if you have a computer that has reached the end of its life and is no longer in use, it's also safer to wipe the hard drive before stashing the machine in a corner or a closet. This can be done easily with a tool such as as Darik's Boot and Nuke ? there are a variety of tutorials on how to use it across the web, (including here).

# Discarding CD-ROMS

When it comes to CD-ROMs, you should do the same thing you do with paper?shred them. There are inexpensive shredders that will chew up CD-ROMs. Never just throw a CD-ROM out in the rubbish unless you're absolutely sure there's nothing sensitive on it.

# Secure deletion on solid-state disks (SSDs), USB flash drives, and SD cards

Unfortunately due to the way SSDs, USB flash drives, and SD cards work, it is difficult, if not impossible, to securely delete both individual files and free space. As a result your best bet in terms of protection is to use encryption?that way, even if the file is still on the disk, it will at least look like code to anyone who gets ahold of it and can?t force you to decrypt it. You can learn about how to use encryption in the [Protecting Files lesson](umbrella://lesson/protecting-files).

Swipe right for this lesson's checklist

### RELATED LESSONS/TOOLS

* [Protecting Files lesson](umbrella://lesson/protecting-files)
* Darik's Boot and Nuke tool guide

### FURTHER READING

* [EFF - How to delete your data securely](https://ssd.eff.org/en/module/how-delete-your-data-securely)
* [Security in a Box - Chapter 6, Secure deleting](https://securityinabox.org/chapter-6)