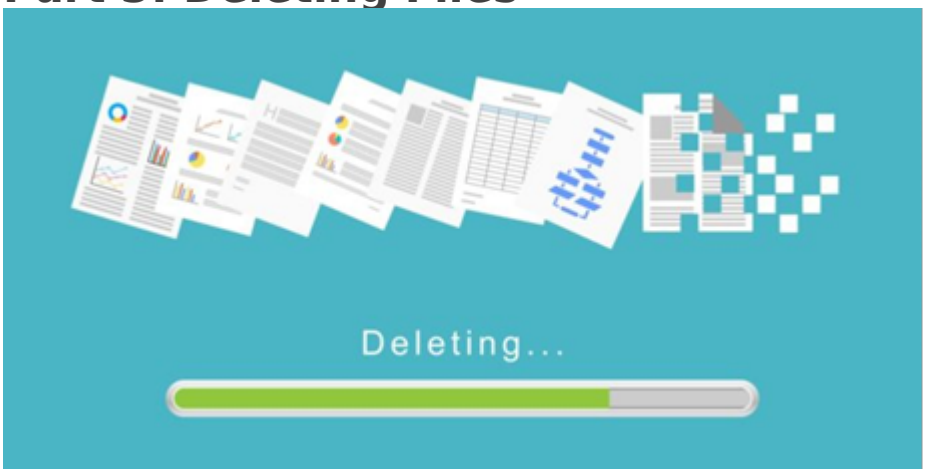
Security Best Practices - Part 3: Deleting Files

Travis - 2021-03-16 - Best Security Practices

Part 3: Deleting Files



TL/DR: Use a secure deletion program that overwrites the data which was deleted with random data.

When you delete a file on a computer, only the reference to the file is removed from the file system table. The file still exists on a disk until other data overwrites it, leaving it vulnerable to recovery.

There are many tools available out there that allow you to securely delete files so they cannot be recovered. This article provides a summary of some of the free tools available out there, many of which are portable, allowing you to securely delete files you may temporarily save to public computers.

Secure Erase on Windows

Eraser

ERASER

- Developer: Heidi
- Open Source: Yes
- Cost: Free

Eraser makes it very easy to securely delete files, folders, or both. It overwrites the files

being deleted with random data. There are several options for the number of times the files being deleted are overwritten with random data, including two versions of the US DoD 5220.22-M standard (3-pass and 7-pass) and the Gutmann method, which overwrites the file with random data 35 times.

You can immediately delete files and folders using the On-Demand interface or schedule files and folders to be securely deleted at a specific time using the Scheduler.

Eraser comes in a version you can install, which also allows you to add an option to the Windows Explorer context menu to securely erase files within Explorer. You can also download a portable version of Eraser you can take with you on a USB flash drive to delete files you save on other computers.

Download the installable version of Eraser from eraser.heidi.ie or the portable version from PortableApps.com.

Secure Erase on MacOS

Apple users have a native secure delete built into the operating system, however, the actual Secure Empty Trash was removed in macOS v10.6.8 and later. That said, however, you can still securely remove files and overwrite them with null data.

On macOS, you can use a command called srm, which can "securely remove files or directories." To do this follow these steps

1. Open Terminal (go to Finder > Applications > Utilities); it's in the Utility folder in your Applications folder,
2. Type the following command: srm -v
3. Type space after the above command.
4. Drag the file that you want to delete into the Terminal window; you'll see that Terminal adds its file path.
5. Press Return and the file will be securely deleted. If the file is very large, this may take a while.

If you want to delete a folder, then use this command:

srm -rv

However, this command may still not delete other copies of a file that had previously been written to other parts of your disk.

Tags

Security