Secure Delete for PC

Secure Delete for PC

Q: How can I securely delete files on a PC?

- How can I ensure a file with sensitive information is securely deleted?
- On a PC, what is analogous to "secure empty trash" on a Mac?
- How can I make sure a Word or Excel file is really gone?

On this page:

Context

On a Windows machines, a simple 'Empty Recycle Bin' will only erase the index to a file, not the file itself, thus exposing you to some risk if the file contained sensitive information, such as SSN, or anything you'd rather someone else could never see. To securely 'delete' a file involves overwriting the file several times. This will take longer than a simple 'Empty Recycle Bin'.

Answer

Via the Windows CMD prompt the Format command's /P parameter can be used (in Windows 8 and 10) . The /P parameter still allows you to specify the number of passes, but now instead of just overwriting the sectors on a disk with 0's, additional passes overwrite sectors with random numbers. Furthermore, the number of passes you specify is in addition to a single pass of 0's.

So, for example, if you were to use the command

```
format F: /P:4
```

drive F: would be formatted and then every sector on the disk would be overwritten once with 0's. Then, the Format command would overwrite each sector four more times; each time with a different random number. Keep in mind that each additional pass you specify will increase the amount of time it will take the Format command to complete its task. This will decrease the likelihood that anyone will be able to retrieve any sensitive data.

There are alternative options to add this functionality to a Windows machine - see Removing Sensitive Data (On a Mac, under 'Finder', there are options for 'Empty Trash' and 'Secure Empty Trash'; secure delete functionality is also part of the IS&T supported PGP encryption implementation)

The information below describes one option: a widely used, free, open source tool called **Eraser**, which can securely erase selected files on a PC. Files are overwritten several times, which means they are virtually impossible to restore. Eraser is not officially supported or distributed by IS&T and advise users to backup all needed data.

The following directions are for a basic file delete functionality on Windows. (Other features of Eraser, such as a scheduling function, or other OS's are not covered here.)

Eraser Setup

1. Close all applications except for the browser.
2. Go to http://eraser.heidi.ie/download.php
3. Download the most recent version by clicking on its name.
4. Open the download.
5. Double click **erasersetup.exe** and select **Run**.
6. The Eraser Setup Wizard opens.
    a. Close any open applications (e.g. the browser).
    b. Click **Next** to continue.
    c. Accept terms of license and click **Next**.
    d. Choose Setup Type **Typical**

    e. Click **Install** and when done installing, click **Finish**.

7. Setup is now complete.

To delete a file

Right click on the file name/file icon and select **Eraser > Erase**.

OR:

Right click on the Recycle Bin and select **Erase Recycle Bin**.

Reminder: A secure delete takes longer than a simple delete; if you have many items in your recycle bin, this could be several minutes.

If you have already deleted a number of files using the conventional 'Empty Recycle Bin', you can improve your security by overwriting all free space. This can take a long time - several hours, and may be an action to start before you go home.

1. Find and open 'Eraser' in the Start menu.
2. Select **File > New Task**, then **Unused space on drive**.
3. Select **Start**.

Optional tweaking of Eraser

1. Find and open Eraser in your START menu.
2. Select the **On Demand** icon on the left.
3. Select **Edit > Preferences > Erasing**. You will see the options for the number of 'passes'. The default is 35, which is relatively slow. You may want to select option 2, which is 7 passes.