How to safely delete sensitive files on Windows 11

When you tell Windows to delete a file, you usually want it gone forever. However, some data recovery applications and services can restore those files even if you think they've been completely deleted.

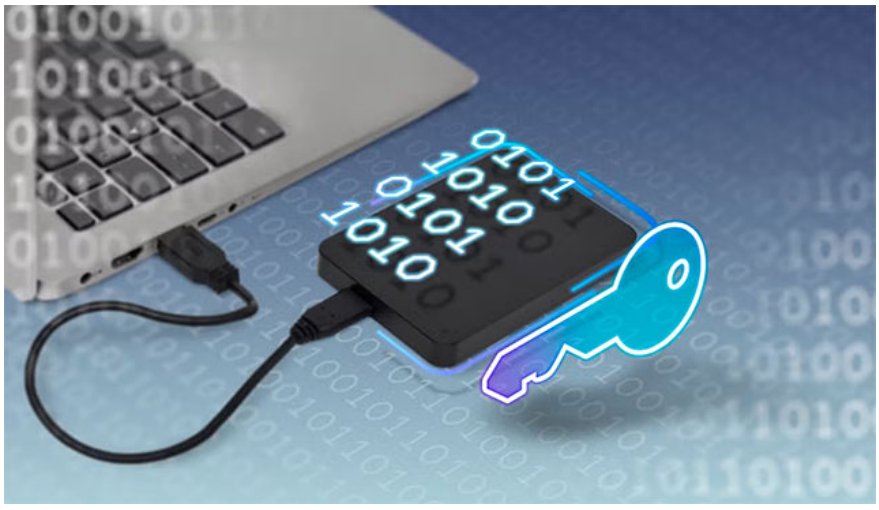
When you tell Windows to delete a file, you usually want it gone forever. However, some data recovery applications and services can restore those files even if you think they've been completely deleted. So it's important to know how to delete these 'sensitive' files completely, permanently, and irrecoverably.

Why 'Delete' but not really delete

In fact, when you delete a file on Windows, it doesn't disappear from your system's hard drive immediately. Instead, Windows marks the file's storage space as free, signaling that it may be overwritten by new data in the future. Until that happens, bits of your file remain on the drive, making it relatively easy to recover them with the right tools and knowledge.

Encrypt files to prevent recovery

An easy way to get around this is to encrypt your hard drive or the individual files and folders you want to delete. You can use Bitlocker or third-party apps like Veracrypt to do the job. This won't stop someone from recovering the deleted data, but it's all useless without the decryption key, so it might as well be 'buried deep'.



Cipher command overwrites free space

Windows has a built-in tool called 'Cipher' that will overwrite all free space with random data. This prevents files from being 'un-erased', although it can take a long time if you have a lot of free space, and you also shouldn't do it on an SSD as it increases wear. Cipher is actually an encryption tool, as the name suggests, but if you use the '/w' switch it will overwrite unallocated space.

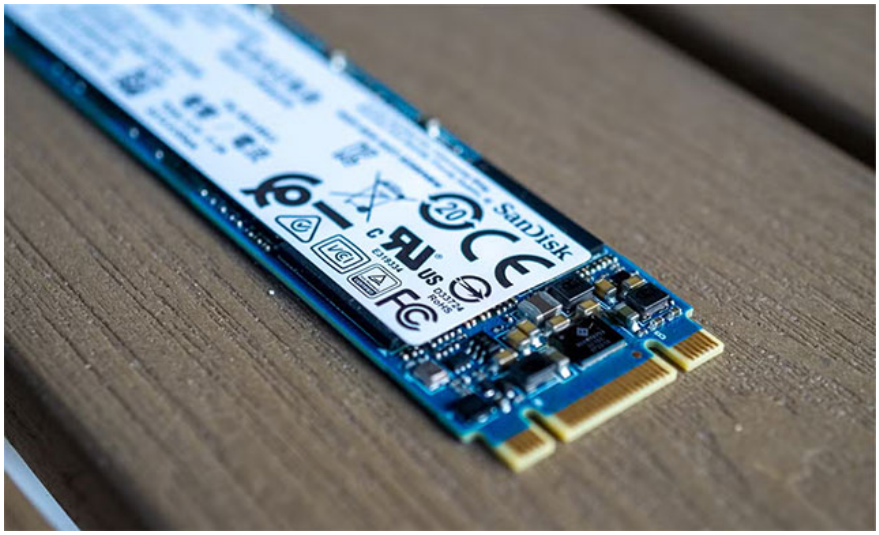
All you have to do is open the Command Prompt or Terminal application as administrator and type:

```
cipher /w:c:
```

This will overwrite all the free space on your C drive. Change the drive letter as needed. You don't have to do this on the entire drive either, using the full path like "C:secretstuff" instead will be faster because it will only overwrite things that have been deleted from that folder. Note that this only works on drives using the NTFS file system.

Securely erase entire hard drive

For SSDs, the best way to ensure data cannot be recovered is to use a 'secure erase' function. The way SSD wipes work (especially the TRIM command) makes it difficult to recover deleted data, but you can sometimes find a secure erase function for an SSD in your computer's BIOS, or even better, use software provided by the drive manufacturer.



For example, Samsung's Magician software offers a "secure erase" option. Before using BIOS or other third-party tools to securely erase an SSD, check to see if the manufacturer provides its own official tool for this purpose.

Try Recovery as a test

An essential check after you've securely erased your hard drive is to try to recover the files yourself. You can use an application like Recuva to check if any of the files are in a recoverable state. You don't have to actually perform the recovery, just check to see if the software finds anything.

You finished reading the article "**How to safely delete sensitive files on Windows 11**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
