

CYBER SECURITY

newsletter

DELETING YOUR INFORMATION SECURELY

Problem

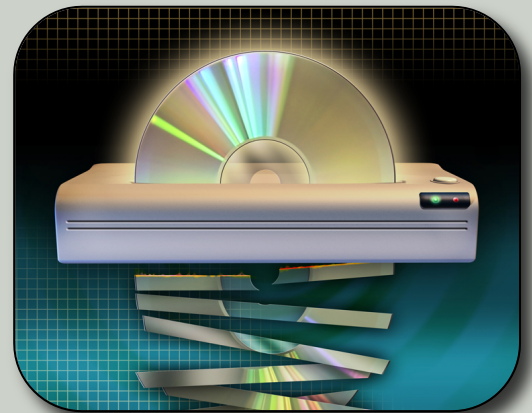
Computers and technology in general allow us to store a tremendous amount of information. Much of this information is very private, such as your work documents, emails, personal photos, or even instant messages or recorded phone calls. Over time, you may find yourself with a great deal of private information that you no longer need. You, like many others, probably just delete the information, believing that once deleted the information is gone and can never be found or recovered. Unfortunately, this is not true.

When you delete information, whether from your computer hard drive, your USB flash drive, or some other device, the files are actually still there. You may think that your private emails or personal photos are safely eliminated, but they are not. Even reformatting the hard drive is not enough to make these files disappear. Deleted files can be easily found and recovered by anyone who has access to the device the data is stored on. If you want to permanently remove your files so no one can ever access them, you will need to “wipe” them from your computer.

Solution

Wiping is a process whereby every byte of your file is overwritten, often with a series of zeros. Once wiped, a file can never be found or recovered, it is gone forever. Wiping usually requires special programs and there are many to choose from.

The reason you need to wipe files is this. When a computer opens or saves your files, it uses something similar to the table of contents found in a book. This table of contents indexes all the files on your computer. When your computer needs to find a file, it looks first in the table of contents. When you delete a file, all that really happens is that your file's entry is simply removed from the table of contents. The file itself is still on your hard drive, but because it is removed from the table of contents your computer thinks it is no longer there. As you use your computer over time, your old, deleted files are overwritten by new files. However, deleted files can still be found and recovered until they are overwritten. Wiping a file ensures that it is overwritten, it is the only way you can be sure that the file is gone for good.



Deleting Your Information

You may not realize it, but when you delete emails, documents and any other files, that information is actually still on your computer. To permanently erase your data requires something called wiping.



University of Colorado

Boulder | Colorado Springs | Denver | Anschutz Medical Campus

This newsletter is published by the University of Colorado Office of Information Security. For more information please send email to security@cu.edu or visit <https://www.cu.edu/information-privacy-and-security>

Recovering Deleted Files

There are a variety of tools and methods that you can use to recover your deleted files. First, when you delete a file on a Windows computer, that information is actually copied to a different part of your computer called the Recycle Bin. The Recycle Bin (or sometimes called the Trash Can, depending on your operating system) is nothing more than just another folder. If you want to recover deleted information, you simply need to open the Recycle Bin and select Restore All Items. Or, if you prefer, you can pick certain individual files to recover.

However, if you empty the Recycle Bin the information cannot be recovered with this method. When you empty your Recycle Bin the information is deleted from the folder and no longer available to you. However, remember that even though the files have now been deleted the files are actually still on your computer. It is only their entry from the table of contents that has been removed. Once again, you can use special programs to find and recover your deleted file.

What To Wipe

When you delete a file, the file itself still exists. One way you can permanently erase private files is wiping. Wiping erases the file by physically overwriting every byte in the file. It is almost impossible to recover a file that has been wiped because the file is no longer there. Wiping is a process that can be performed on any device that stores information. We all have private files on our computer that we want erased for good. These are files you should wipe, rather than simply delete. Other devices you may want to consider wiping include:

- USB Flash Drives
- Camera Memory Sticks
- Backup Tapes
- Smartphones

Options For Wiping

Not only can you wipe different devices, but there are different ways you can wipe your data. Choose the method that works best for you. Your choice will depend on the amount or type of data you have to erase.

By File: With this method, you can choose to wipe an individual file, multiple files or entire folders instead of simply deleting them. Depending on the program you are using, you may have a special trash bin provided just for the purpose of wiping files.

By Deleted Space: With this method your computer wipes all previously deleted files on your drive. In other words, everything that you deleted in the past, but can still possibly be recovered, is securely wiped. This ensures that these documents can never be recovered.

By Drive: With this method, you can wipe an entire drive. This is often done when you want to dispose of an old computer, sell a used laptop or perhaps give someone your old USB memory stick. There is a tremendous amount of data stored on the device, both deleted and active. The only way you can safely erase any sensitive information is to wipe the entire hard drive.

Multiple Wipes

Different wiping programs provide you with different options. Most of the programs allow you to wipe files several times. Simply overwriting a file once is usually enough. However, in situations where security is very important, and you have time, you can overwrite your files multiple times. However, depending on the amount of data you have, wiping can take a long time. Wiping can take several hours if you have gigabytes of data, it can take even longer if you are wiping your entire hard drive.