CYBER SECURITY Newsletter

PERMANENTLY ERASING DATA

Problem

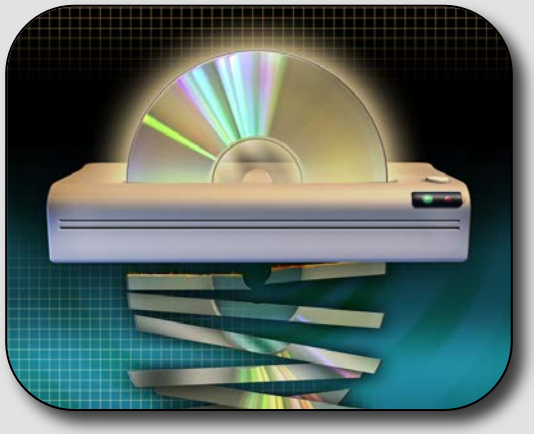
Computers and technology allow us to store a tremendous amount of information. Much of this information is very sensitive, such a work documents, emails, personal photos, instant messages and recorded phone calls. Over time, you may find yourself with a great deal of sensitive information you no longer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

When you delete information from your computer hard drive, mobile device or USB flash drive the files are still there. You may believe these files are safely eliminated, but they are not. Even reformatting the hard drive is not enough to remove the files. 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 erase your files so no one can ever access them, you will need to "*wipe*" them from your computer.

Solution

Wiping is a process where 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 your computer confirms all your files have been permanently deleted and the information remaining on your computer is secure.

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 your file's entry is removed from the table of contents; however, the file itself is still on your hard drive. Even though it was removed from the table of contents your computer thinks it is no longer there. As you use your computer over time your old and deleted files are overwritten by new files. However, as long as your deleted files have not been overwritten by new files, they can be found and recovered. Wiping a file ensures that it is overwritten; it helps ensure that the data is gone for good.



Erasing Your Data

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

JUNIATA COLLEGE

This newsletter is published by Campus Technology Services. For more information please contact us at:
help@juniata.edu

Recovering Deleted Files

There are a variety of tools and methods you can use to recover your deleted files. When you delete a file on most Windows or Mac computers that information is actually copied to a different part of your computer called the Recycle Bin. The Recycle Bin (or called the Trash Can on Mac OS X systems) 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 you can pick certain individual files to recover.

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

What To Wipe & How

You may be surprised at where sensitive data may be stored. You most likely have sensitive data on your computer and other devices. You may want to consider wiping these devices:

- Copier hard drives
- Tablets
- USB Flash Drives
- Camera Memory Sticks
- Backup Tapes
- Smartphones

Depending on your operating system, your computer may already have an option to securely wipe data (often called secure deletion). If your device does not have a wiping option then you will need to use a special program to wipe the sensitive data. To learn more about tools for wiping, contact the help desk or security team.

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 need to erase.

1. By File

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

2. By Deleted Space

With this method your computer wipes all previously deleted files on your drive. Everything you deleted in the past, but can still possibly be recovered, is securely wiped. This ensures these documents can never be recovered.

3. 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.

Multiple Wipes

Different wiping programs provide you with different options. Most wiping programs allow you to wipe data multiple times. Simply overwriting a file once is usually enough. However, in situations where security is very important you may want to overwrite highly sensitive data multiple times. Keep in mind the more data you have, and the more times you wipe it, the longer the process can take. If you attempt to wipe Terabytes of data using multiple wipes, this process could take many hours if not days.