Destroying Information

Digital information is stored on every device you use, including a computer but also removable devices such as USBs, CDs, and DVDs. These devices save a great deal of information without your knowledge. This data, along with the sensitive information you intentionally put on a device, can be harmful if individuals with malicious intent get ahold of your device. This is why it is crucial to securely manage your digital information. Tools such as **Eraser** and **CCleaner** securely and permanently delete information.

There are **security threats** that necessitate the use of **Eraser** and **CCleaner.** Information that you think you have deleted is actually still on your computer, and easily recoverable. Until data is *wiped*, or securely erased, the information remains and can hurt you!

There is no such thing as a delete function. When you simply "delete" a file, its label is removed and Windows knows that the space can be used for something else. But until the space is actually used for something new, the contents of the "deleted" file remain. Even if you "delete" a file and empty the trash, the data remains.

Every time a document is saved, a new copy of the document is created. By the time a document is finalized, you could unknowingly have several versions of it saved on your computer.

Recovery of "deleted" documents can be quite easy with the right software. Consider if someone stole your computer. Because information is never really deleted, the thief would see a great deal of information—sensitive and non-sensitive—that you thought you deleted.

For these reasons, you should *never trust the delete function on any device*. The *only* way to securely and permanently delete a file is by **wiping** it. Wiping replaces or writes over the data. But even data that has been wiped once can be recovered and read. Effective data erasing programs overwrite your data multiple times. The more times data is overwritten, the less likely it can ever be recovered. Three or more overwrites is sufficient, although some standards recommend seven or more.

Eraser permanently wipes **deleted files**, contents of the **recycle bin**, **free disk space,** and other **existing files** you instruct it to wipe. Eraser can run on-demand or on a schedule. *Wiping an existing file will only delete the most recent version, so if the file has been modified in the past, the past versions will not be wiped*.

To erase previous versions, you will need to wipe the **free disk space**. When files are deleted with the Windows function, and emptied from the recycle bin, they are stored on the unallocated space on your drive. Wiping the free disk space will get rid of these files but not any existing (saved) files. *Anything saved on your device will not be wiped unless you select the individual files for wiping, or move the files to the recycle bin and empty the recycle bin.* This is why it is crucial to know what information is stored on your device; no tool can help you if you do not know where your sensitive info is!

CCleaner wipes the most common **temporary files**. These files are a threat because default computer and Internet browser settings automatically collect and save data on your activities. Every time you use Internet browser, word processer, other common programs, temporary files are created with sensitive data. It is important to securely erase this data because it gives away a lot of details about your activities and work.

Temporary data includes:

- Browser records of personal data, account information, browsing history, cookies, etc.
- Temporary files saved by applications for recovery; lists of recently viewed documents
- Files and links used as shortcuts
- Windows **swap file**: a file of current data created by Windows when the computer's memory is at capacity

CCleaner can also wipe **free disk space** and the **Windows Registry**, which includes information on your computer configuration, hardware and software settings, etc. Using CCleaner will not only make you more secure, but will improve the speed and functionality of your computer

If you are discarding a CD, DVD, or other removable disk, it might be easier to break the device rather than wipe it, since it requires a significant amount of time and technical resource to gather information from a disc broken into many pieces. But it is possible, so use your judgment.

Remember:

- Once a file is wiped with Eraser or CCleaner, you will not be able to recover it.
- Before wiping any data:
    - Create an encrypted backup of important files
    - Delete all unnecessary files and empty the recycle bin (thus moving these files to the unallocated space on the drive).
- To maintain the security of your data, wipe sensitive files immediately and wipe your entire disk periodically.

RESOURCES

- **Tools**
    - **Eraser:** www.heidi.ie/eraser
    - **CCleaner:** http://www.piriform.com/ccleaner

- **Security-in-a-Box**
    - **Destroying Sensitive Information:** https://security.ngoinabox.org/en/chapter-6
    - **Eraser:** https://security.ngoinabox.org/en/eraser_main
    - **Portable Eraser:** https://security.ngoinabox.org/en/eraser_portable
    - **CCleaner:** https://security.ngoinabox.org/en/ccleaner_main
    - **Portable CCleaner:** https://security.ngoinabox.org/en/ccleaner_portable

- **Tech4Net**
    - **General Resources:** http://tech4net.org/?page_id=12