Effectively Erasing Files

Where do deleted files go? When you delete a file, depending on your operating system and your settings, it may be transferred to your trash or recycle bin. This "holding area" essentially protects you from yourself—if you accidentally delete a file, you can easily restore it. However, you may have experienced the panic that results from emptying the trash bin prematurely or having a file seem to disappear on its own. The good news is that even though it may be difficult to locate, the file is probably still somewhere on your machine. The bad news is that even though you think you've deleted a file, an attacker or other unauthorized person may be able to retrieve it.

What are the risks? Think of the information you have saved on your computer. Is there banking or credit card account information? Tax returns? Passwords? Medical or other personal data? Personal photos? Sensitive corporate information? How much would someone be able to find out about you or your company by looking through your computer files?

Depending on what kind of information an attacker can find, he or she may be able to use it maliciously. You may become a victim of identity theft. Another possibility is that the information could be used in a social engineering attack. Attackers may use information they find about you or an organization you're affiliated with to appear to be legitimate and gain access to sensitive data.

Can you erase files by reformatting? Reformatting your hard drive or CD may superficially delete the files, but the information is still buried somewhere. Unless those areas of the disk are effectively overwritten with new content, it is still possible that knowledgeable attackers may be able to access the information.

How can you be sure that your information is completely erased? Some people use extreme measures to make sure their information is destroyed, but these measures can be dangerous and may not be completely successful. Your best option is to investigate software programs and hardware devices that claim to erase your hard drive or CD. Even so, these programs and devices have varying levels of effectiveness. When choosing a software program to perform this task, look for the following characteristics:

- **data is written multiple times** - It is important to make sure that not only is the information erased, but new data is written over it. By adding multiple layers of data, the program makes it difficult for an attacker to "peel away" the new layer. Three to seven passes is fairly standard and should be sufficient.
- **use of random data** - Using random data instead of easily identifiable patterns makes it harder for attackers to determine the pattern and discover the original information underneath.
- **use of zeros in the final layer** - Regardless of how many times the program overwrites the data, look for programs that use all zeros in the last layer. This adds an additional level of security.

While many of these programs assume that you want to erase an entire disk, there are programs that give you the option to erase and overwrite individual files.

An effective way to ruin a CD or DVD is to wrap it in a paper towel and shatter it. However, there are also hardware devices that erase CDs or DVDs by destroying their surface. Some of these devices actually shred the media itself, while others puncture the writable surface with a pattern of holes. If you decide to use one of these devices, compare the various features and prices to determine which option best suits your needs.