Title:
How To Wipe Disk Drives, And Why

Word Count:
517

Summary:
Data security has become a bigger concern as the information age goes into full swing. Computers are becoming more and more commonplace as versatile tools for a wide variety of tasks and uses. This has made digital storage increasingly the data storage format of choice, since digital information is easily accessed and processed by computers.

This has led to a rise in interest in digital information and data storage systems. Apart from developments in hardware technology th...

Keywords:
wipe disk,disk wiping,wiping hard disk

Article Body:
Data security has become a bigger concern as the information age goes into full swing. Computers are becoming more and more commonplace as versatile tools for a wide variety of tasks and uses. This has made digital storage increasingly the data storage format of choice, since digital information is easily accessed and processed by computers.

This has led to a rise in interest in digital information and data storage systems. Apart from developments in hardware technology that allow bigger capacity devices with faster access times, security has also become a prime consideration. Most software and programs nowadays come equipped with varying levels of security options. For instance, it is now possible to protect almost any file with a password such that only those who can provide the correct password would be able to access the information within the file.

However, these software security measures would not stand up to dedicated data extraction efforts, in particular those involving the actual physical hardware. Physically securing the hard drive (or other data storage device) under consideration may not always be possible or practical. Another way of ensuring that important data is not placed at risk is to wipe the disk.

Simply deleting the contents of a hard disk is not enough to ensure that they

are not recovered. In fact, there are software utilities that allow the recovery of deleted data. This possibility is because when a file is deleted, it is not actually overwritten or removed from the hard disk. Instead, a marker is just associated with the file to say that it has been deleted, and the space it occupies on the disk is marked available for use. This means that the data in the file remains on the disk for the knowledgeable hacker to extract and view.

Wiping a disk, on the other hand, is a much more thorough process. In a disk wipe, all data to be wiped off is actually overwritten with random data. This eliminates almost entirely the traces that a normal deletion leaves behind, and makes recovery of data practically impossible. (In theory, it would still be possible to reconstruct the data lost after a hard disk wipe, but this would require high-powered microscopes and would proceed much too slowly to be useful!)

Performing a disk wipe is facilitated by the many disk wipe programs available. There are many free options, as well as commercial software options, which may differ in terms of functionality and documentation. The majority of these are available online, which makes it quite easy to browse through and find the most appropriate program for the specific task. Some programs are designed for use on a single personal computer, while others may be designed for use on batches of computers.

Confidential data that needs to be kept from being exposed may best be hidden by using a disk wipe. This simple additional security measure makes the recovery of deleted data nearly impossible. With the many disk wipe programs available, it is easier than ever to perform a disk wipe, even for casual users, making this a real data security option.