

Security of USB Flash Drives

Contributed by admin
Sunday, 09 November 2008

Even the biggest USB flash drive is still smaller than most people's thumbs. Since we carry these devices to numerous locations, there is a fairly good chance that we will eventually lose them. If this should happen, most of us simply hope there was nothing sensitive on the drive. However, that is not the only thing you can do. There are some basic USB flash drive security measures available.

If your flash drive carries some sensitive information that you hope to keep from ending up online by the next day, security measures available range from secure partitions to encryption options. Secure partitions are a rudimentary form of security - a password protected partition is created on the drive, using a utility supplied by the manufacturer, this makes a public partition and a secure one.

In most cases, it is not possible to access these partitions at the same time, it is often necessary to log into the secure partition, hiding the public one. Not all controllers feature this limitation. Using a version of your utility, someone else could re-partition the drive. However, they would not have access to the data you have stored on the secure partition.

There are other USB flash drives that are much more specialised, they offer the same sort of secure, password protected partition. However, they also encrypt data stored on that partition, making it much harder for people to get to your data. While encryption algorithms can be broken, having encryption on your USB drive is an extra layer of security you can offer your data.

The down side to drives that use encryption is that some of them only perform this encryption in software that results in lower performance on the drive when encryption is enabled. Few manufacturers use a hardware based engine capable of encrypting and decrypting files at a higher speed to prevent performance penalties when you access a secure partition that's using encryption.

The problem with both of these security approaches is that they are mostly dependent on software; the majority of manufacturers of USB flash drives only provide Windows based software support.

What does that mean for Macintosh users and people who use a Linux distribution or other unusual operating system? Security for USB flash drives is mostly still a matter of keeping good track of them. While it is possible to access public partitions on almost all systems, accessing the secure partition generally requires access to Windows.

USB flash drive security is still in its infancy, since these drives aren't routinely used by people with a need to secure their data. As they become more widespread and the need for security increases, expect flash drive security options to increase as well. For now, partitioning and encrypting are the major options available, though.

Windows users are in luck and can make use of both of these options effectively to preserve their data. However, users of operating systems that aren't compatible with the software on the drive must simply try not to let their USB flash drives fall into the wrong hands.