Flash Drives and the problems of traveling salesman

WinEncrypt

WinEncrypt™

Flash Drives and the problems of traveling salesman

A true contingency problem arises whenever a person tries frantically to protect the data that is in one or more ways important. The range of the people might vary from a school going teenager to a corporate hotshot. People dealing with a lot of files are always losing their sleep over how to protect the data and keep the information safe and sound. There have been numerous attempts to safeguard the data and protect any flash drives from virus and Trojan attacks but most have proved to be untrustworthy.

Flash drives are the most vulnerable of the transfer mediums although they might come packaged with encryption software. The traveling salesman would always be the one who would sweat more and more with the failing of the USB encryption to protect the data that is being carried to places. One might even say that the encryption techniques have not been able to stay updated with the new and new kind of attacks that are registered each and every day. But that would be undermining the lot. Flash drives travel to various machines from where the information again goes to other machines. This makes them a recipient of a lot of different technological environment and the encryption softwares might just interfere with the working mechanism of the machine whereby the user himself might jut disable the windows encryption option leading the flash drive open to threats.

It should always be kept in mind that the encrypted drive must be respected if one wants to not lose the information that is stored there. The sensitive information that might range from important certificates to financial statistics to databases might just get corrupted if proper action is not taken. The traveling salesman must also carry with him the proper antivirus or the encryption software that would be able to relieve him of the problem of corrupted data. Trojans are the most disruptive element as they are found in plenty and easier for the hackers to create. While downloading some information off the internet, one should be fully sure with proper anti spyware or anti malware software that would guarantee the restriction o the spywares and the Trojans. The flash drives get the maximum amount of the attacks from the internet whether or not any information is being exchanged in that particular machine. Be sure of the encryption software that you are using with the USB drive. Data can be secured on the CD or DVD that one uses but the importance of the flash drive is unique as that is the fastest data transfer methods possible for large files.

The encryption software must be made compatible to different working environments and the antivirus software that is being used must be able to delete any kind of threats that the flash drive might face. The files and folders, after encryption, also become very sheltered for the traveling salesman and if password protected then it becomes even more secure.
So who can benefit the most from this system? No wonder all and any of us, but especially companies dealing with finance and outsourcing have been using these systems the most often to secure their targets and networking. Healthcare sectors, one of the most interfered of departments in the security area, have now been a keen follower of this system. Personal as well as sensitive information are kept under security check while it is made sure that no one else can access through your security numbers or passwords.

WinEncrypt™

CryptArchiver: Protects files on PCs & USB Drives

- Keep your important files away from prying eyes.
- Create virtual "Encrypted Drives" upto 20 GB in size.
- Uses strong 448-bit Blowfish and 256-bit AES encryption.
- Easy to use, just drag-and-drop!
- Password-protects all types of files and folders.

Read more about free encryption software at WinEncrypt.com