LIFE GOES ON BAG - ENCRYPTION 101

Workbook page: None
Listening to Katrina companion page: HYST - Documents

You are going to scan all your pictures, vital records, and other documents and store them digitally. (Things that are already digitized, like photos from your digital camera, will not need to be scanned.) The danger in doing this is that if someone steals your laptop computer, they will have full access to your personal information, and identity theft is all too common these days.

We need to have a way to deny anyone but ourselves access to our vital information. The way to do that is to use a technology called encryption. Encryption software uses complex magic-like processing to turn all of your data into scrambled gobbledee-gook. The software can also turn the gobbledee-gook back into readable data - but only if you know the right code. Essentially encryption allows us to create a special kind of folder on our computer the contents of which are accessible only to us. It's like a safe for your software.

If you want to learn more about encryption technology, you can type it into Google, and you will have weeks worth of reading material. For now, I'm just going to tell you how to use it.

In order to work this magic, you will need some software - some of which is very expensive. Since I am the cheapest man alive, I prefer things that are cheap or free. If you are like me, then TrueCrypt is the product for you. Go ahead and visit the website now by clicking on the TrueCrypt link. In the toolbar, click the **DOWNLOADS** link and then download and install the latest version. (I am going to assume that you are computer savvy enough to download and install small programs on your own. If you aren't, then you need to get a kid to teach you.)

Once you've got it installed, click the TrueCrypt icon on your desktop to open it. Click HELP in the menu at the top, and then select User's Guide This will open the User's Guide, which will teach you how to use the program. You will want to create encrypted file containers using TrueCrypt, and store your vital documents inside these containers. TrueCrypt is a powerful tool and can be used to create other types of encrypted volumes, but the file volumes are portable - that is we can copy them to other places and make backups of them easily.

Everything is laid out very well in the User's Guide, so I won't waste time on re-documenting the process. Once you have created and mounted your encrypted volume, you can move things into it. Here you can see that inside my encrypted volume I have everything that was once in my Documents folder. Now it is all protected by TrueCrypt.

If you look at the folder structure we previously created, all you see in the Documents folder is the TrueCrypt volume file named 'memdump'. You can name your volumes whatever you like.

In the MemKeys folder, I made a folder for my first Flash Drive called MemKey1, where I copy the 'memdump' TrueCrypt volume for replication to the Flash Drive.

You can see that I have also used the TrueCrypt 'Traveller Disk Setup' to create a portable version of TrueCrypt which also comes along on the Flash Drive. You can read about how to do this in the User's Guide.

Shane Steinkamp © 2008 - All rights reserved.

You can create other encrypted volumes for other things if you like. You can create a different one for every member of the family. I prefer to keep everything in one file and replicate it for each family member. Of course, only my wife and I know the passwords, but as the kids get older they will need their own volumes for their things. You will need to modify the configuration of your data store as needed.

The TrueCrypt volume files are very secure - as long as you have used a good password - and you can safely copy that file anywhere - onto your backup drive, onto your USB Flash Drive, or even upload it to a remote server on the internet. It is totally portable. You obviously see where this is going. You can tie that USB Flash Drive around your neck like a necklace, run out of the house otherwise naked, and you'll have a copy of every vital document. The value in that is tremendous.

Now that you have your data store configured, and you have your encryption in place, it's time to put some wealth into that bank. That's the subject of the next page.

Shane

Shane Steinkamp © 2008 - All rights reserved.