(Approx. 632 words)

Dan’s Desk

Encrypting a Drive

By Dan Douglas, President Space Coast PCUG, FL

March 2019 issue, The Space Coast PC Journal

www.scpcug.com

datadan (at) msn.com

Last month I described a BIOS password problem that I had to solve. This month, we’ll look at other password locks such as those used for protecting hard drive data.

One of the added features of Windows 10 Pro over the Home edition capabilities, is the ability to encrypt a drive to protect all data and files contained on that drive from unauthorized access. An administrator can select a drive from the File Explorer app and turn on the BitLocker option from the right mouse button option list. The user must then select an encryption key using any combination of uppercase and lowercase letters, numbers or symbols up to 64 characters long. It is critical to record this password as it will be impossible to access the files afterwards without this key. Windows will prompt you to save this key on your cloud account, or in a file or by printing it before encrypting the drive.

I recently had a customer who had a broken Surface PC and needed to recover some business files from the drive. The first place they’d taken it to had told them that it was not possible to access the data, not because it was encrypted, but because the drive was a solid-state circuit board, as is usually found in tablets and many Macs, and did not have the usual SATA drive connector. Having used many drives of this type before, I had the correct adapter to convert it to a SATA type connector. That was when we discovered that it had been locked using BitLocker. It prompted us to enter the key and the owner had no idea what that key may be. I told them that without the key I could not access the data for them. They were advised to check all of their paperwork to see if it was recorded somewhere. Fortunately, when the PC was purchased, the BitLocker key was written on their bill of sale by BestBuy! When they returned later with the key, we were able to access the data and transfer the files to a USB stick.

If you need to encrypt just specific files or folders and not a complete drive, there are several alternatives available. For example, Word and Excel provides for the ability to protect a document by applying the ‘protect document’ option to the file through the Word or Excel options. Adobe Acrobat can also be used to protect PDF type files. In certain versions of Windows, namely Windows 10 Pro, Windows 7 Professional, Windows 7 Ultimate, Windows 7 Enterprise, Windows 8 Pro or Windows 8 Enterprise also come with an Encrypting File System (EFS), which lets you encrypt any kind of file, as well as whole folders and subfolders. Users with a Home edition of Windows will need to use either the Office Suite encryption or a third-party solution, such as TrueCrypt, VeraCrypt or 7-Zip. EFS is applied by selecting the folder or file, select the properties/advanced through a right button click, and then select the ‘encrypt contents to secure data’ option. This encryption is applied using the logon ID and password so it is not as secure as that used by the BitLocker and I’m not sure what would happen if the password used by that ID was removed using a password removal tool. Possibly the data would stay encrypted and still require the original password to allow the files/directories to be accessed.

Many USB drives also offer their own encryption system for the files on that drive, but I would be hesitant to use these as the proprietary nature of the program may cause problems later.