

TRUECRYPT

Il miglior modo per proteggere sia i computer che altri dispositivi di memoria come pendrive; memorie flash in generale, cd, dvd ecc. è come prima detto l'utilizzo della crittografia. Il programma che consiglio di utilizzare si chiama **TrueCrypt** ([Download TrueCrypt](#)) .

Questo software ci permette in modo del tutto gratuito di rendere i nostri dati inaccessibili se non

si è a conoscenza della password. Permette infatti di creare dei file sui nostri dispositivi che sono

dei veri e propri hard disk virtual ; consente nelle ultime versioni di crittografare un intero disco rigido

oppure di nascondere un sistema operativo.

Per **creare un' unità disco virtuale cifrata con TrueCrypt** basata, dopo aver ovviamente installato truecrypt andare su:

Cliccare su Tools

Volume creations Wizard

Create a file Container

Standard True Crypt volume

Inserire il nome del file ad esempio **C:\sicuro.tc**

Scegliere l'algoritmo di crittografia consiglio Serpent-TwoFish-Aes che sono tre algoritmi concatenati ma andrebbe bene anche solo [AES](#) anche per una questione di velocità

Scegliere la dimensione del disco virtuale cifrato ad esempio 1024 MB

Scegliere una password lunga e complessa con simboli, lettere minuscole e maiuscole e numeri,

è possibile utilizzare anche un keyfile, come un'immagine ecc, ma se quel file per qualsiasi motivo

viene modificato o perso non sarà più possibile accedere al disco virtuale.

Scegliere il file **System** e cliccare su **format**

Il vostro volume è stato creato

Andare in **C:\sicuro.tc** e cliccare sul file

Si apre una finestra di trueCrypt cliccare su **Mount**

Al computer si aggiungerà un nuovo hd delle dimensioni che avete scelto e sarà praticamente inaccessibile a chi non ha la password. Il volume creato è possibile copiarlo in una memory card

, memorizzarlo su un cd/dvd . Qualcuno potrà dire "si ma devo avere installato anche truecrypt per

usarlo", in realtà truecrypt permette due modalità di installazione quella sul sistema operativo e una

stand alone che permette di copiare i file del software nell'unità in cui è presente il volume crittografato

in questo modo se siamo a casa di un amico con la nostra pendrive crittografata ci basta aprire la

pendrive cliccare su truecrypt e selezionare il **file cifrato** inserire la password ed accedere alle

informazioni sensibili .

TrueCrypt consente di crittografare l'intero contenuto di un harddisk o di una qualsiasi unità di memorizzazione.

Consente la creazione di **dischi virtuali crittografati** (virtual encrypted disk) , Un utente comune vede questi

dischi come semplici file ma basta aprire il file con truecrypt ed inserire la password per vedere una nuova unità

aggiungersi al vostro computer.

TruCrypt Consente di **crittografare intere partizioni** (entire partition or storage device) su memorie Flash USB

e su harddisk

Permette di crittografare partizioni in cui è installato un sistema operativo, in questo caso all'avvio del sistema

richiede una password.

TruCrypt adotta anche delle contromisure nel caso in cui una analisi volta a cercare dati crittografati tenta di

identificare unità virtuali e sistema operativi.

Questa funzioni sono quelle della **plausible deniability** che consentono le **modalità di Hidden** volume che permette

di nascondere un volume crittografato e hidden operating system che consente di nascondere un intero sistema operativo.

Queste funzioni sono ottime se qualcuno tenta di estorcervi la password, in questo modo dando la password del

volume protetto con queste opzioni verrà aperto il volume cifrato con dati fittizi.