Create A Secure Hiding Place For Electronic Documents

This post may contain affiliate links. Thank you for supporting Self-Reliant School with your purchases.

APRIL 22, 2015

It's always a good idea to carry your important documents in your bug-out oreveryday carry bag, but do you want to take the chance of having every piece of your identity stolen if your bag was lost or taken from you? Think about it, you could lose driver's licenses, passports, credit cards, medical records, and lots more! Wouldn't you rather have a way to keep all your important paperwork together in a secure hiding place where, if you lost it, you could rest assured knowing no one else would be able to get to the contents?

In this post I'm going to walk you through creating a super-secure document storage system on a simple encrypted USB thumb drive, one that can't be opened by anyone but you. Even if someone else were to open it, they wouldn't be able to locate your documents. This is a different type of blog post than I usually write - more technical - but stick with me, I'll take you step by step!

Encryption is defined as "*the conversion of electronic data into another form, called ciphertext, which cannot be easily understood by anyone except authorized parties*". This is more than just putting a password on your computer - you

are actually changing the physical structure of the data itself, all those little bits and bytes. If someone gets their hands on the data, but not the "key" to decrypt it, it will just be meaningless gibberish.

There's always an argument over whether any data can be made completely, totally, 100% secure. The method I'm showing you here will protect your documents from various prying eyes, bad guys, local law enforcement, etc. If you've got huge goverment agencies with three-letter names after you, they probably have the supercomputer power to crack this if they get their hands on it.

We're going to be using a piece of software called TrueCrypt. If you've ever worked with computer encryption, then you may know that this program was "retired" in the summer of 2014, and is no longer supported by the authors. Some people go so far as to say it is now insecure. But if you read this article, you'll see that it's still safe to use; even Amazon is currently using it!

One thing I like about TrueCrypt is that it lets you create two "containers" of encrypted files - the main container, and then a second hidden container, each with their own password. This is useful if your thumb drive falls into enemy hands and you are forced or coerced into giving up your password.

If you simply lost your USB drive somewhere and someone found it, it would be secure because of the encryption, and the fact that they wouldn't have the password. But what if your drive was taken from you, and you were asked for the password? You can't just think "Well, they don't have the password, so I'm safe" - a judge could force you to reveal it or hold you in contempt, and someone on the other side of the law could simply beat it out of you.

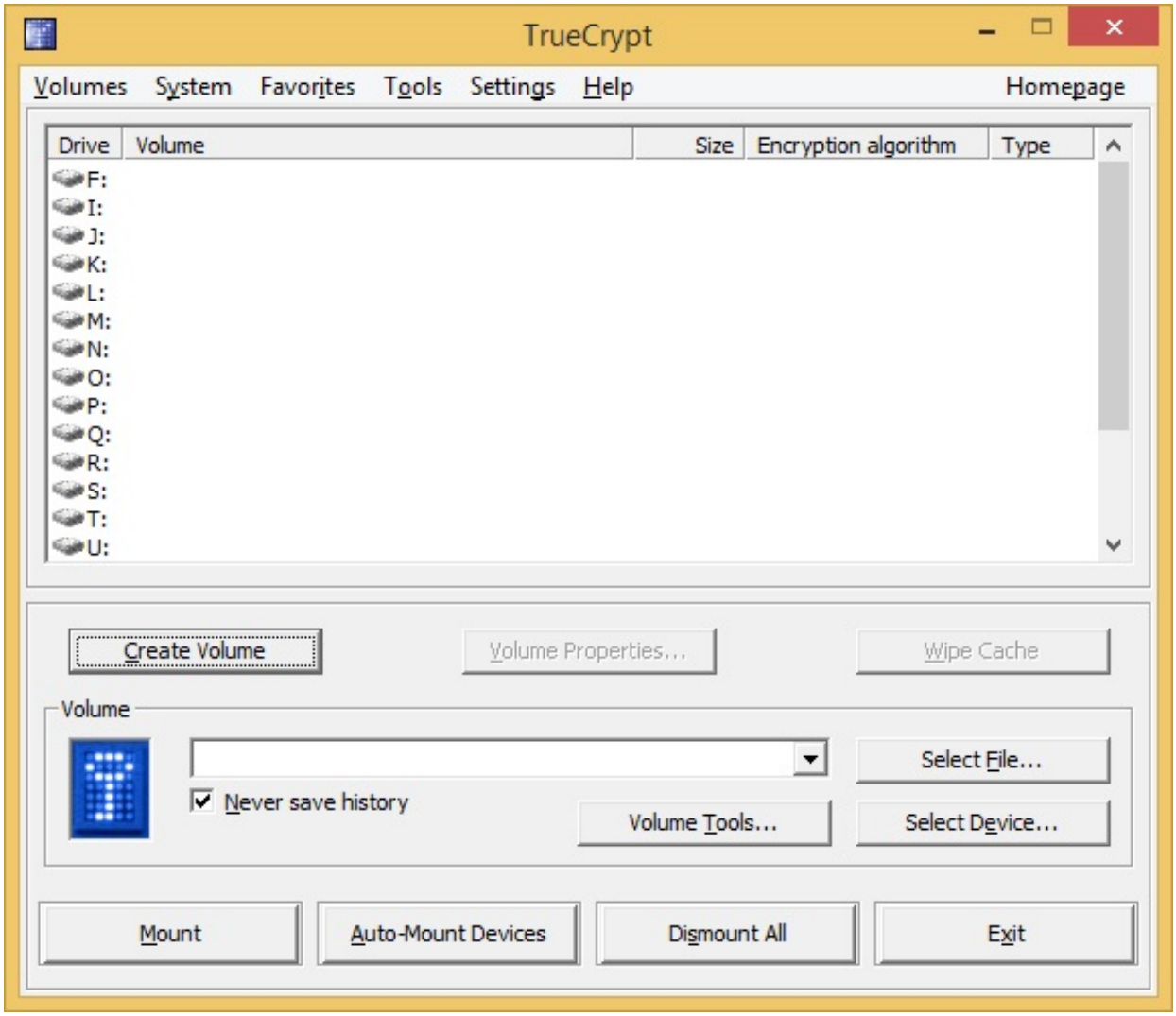
This is where the hidden container comes in. You put your most secure documents in there, and everything else in the main container. If you have to give up your password, you just give up the one to the main container. The bad guys open it and can see the documents you're not worried about, without ever knowing there's another layer hidden below that!

How To Create A Secure Hiding Place For Your Electronic Documents

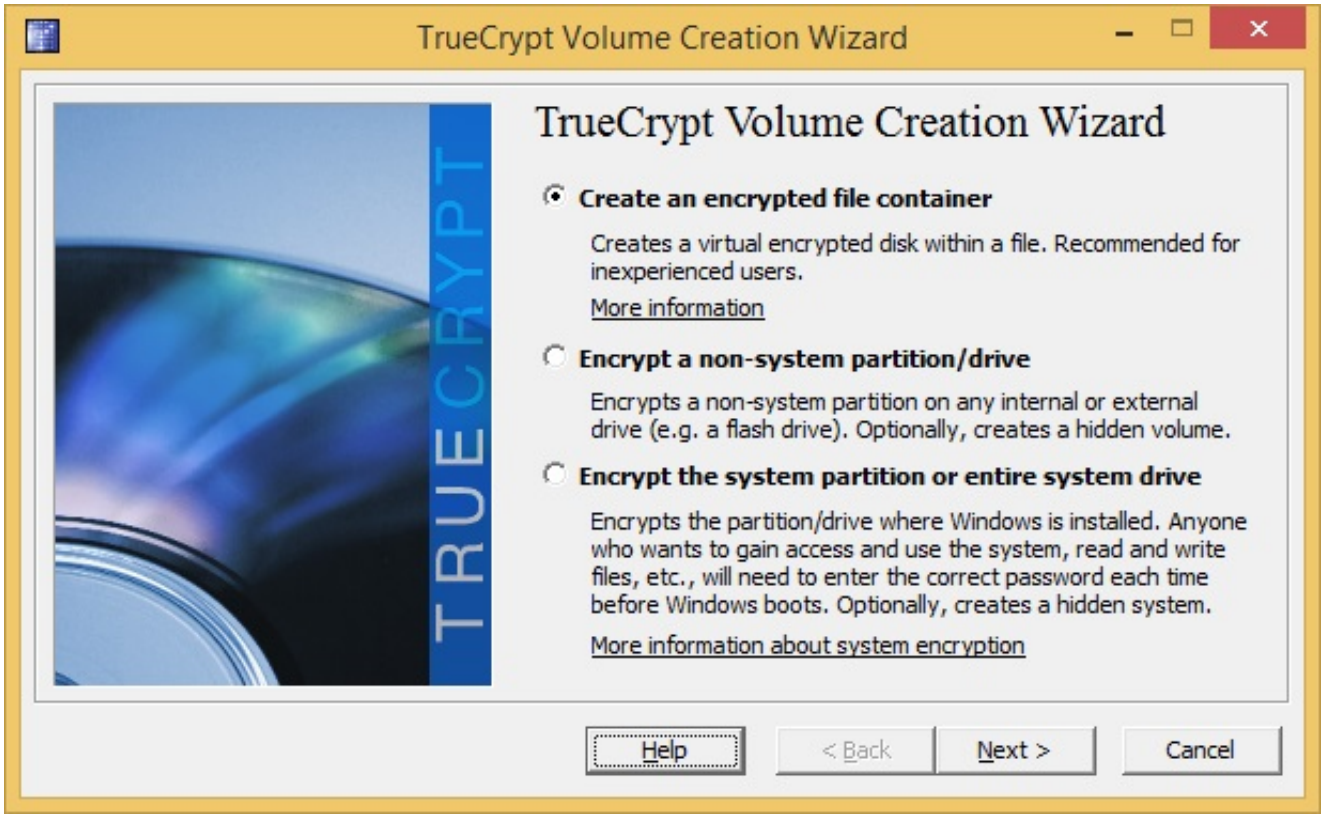
First, you'll need a thumb (USB) drive. You probably already have at least one at home, but if not, they're very cheap. You might even consider getting a aruggedized USB flash drive that resists heat, water and impacts; at the time I'm writing this you can pick up a 16 gig thumb drive for about 10 bucks.

Once you have your USB drive, plug it into your computer. It will have a new drive letter assigned (something other than C: or D: probably). Open the drive, and if it came with any files on it, go ahead and delete them.

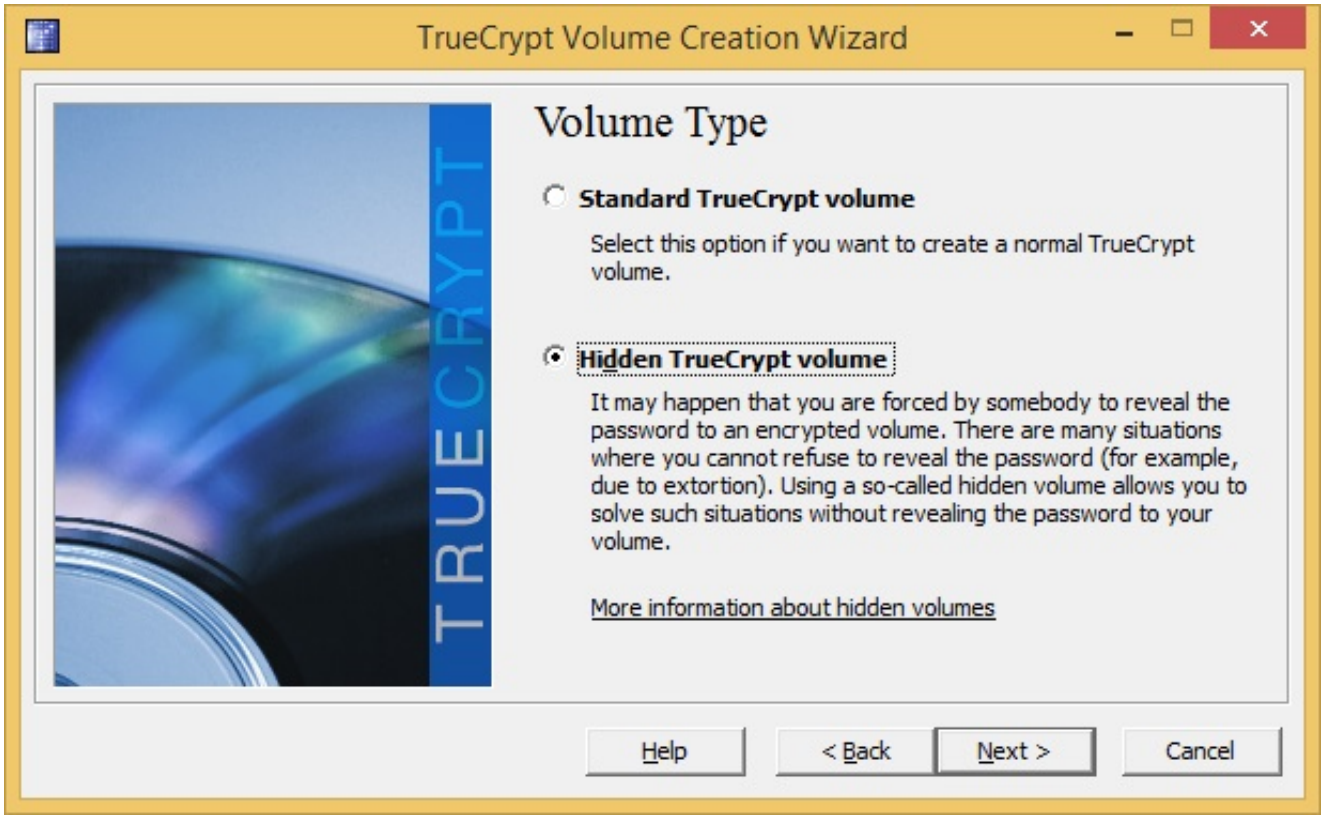
Next, you'll need to download and install the TrueCrypt software. You can download it from this page: https://www.grc.com/misc/truecrypt/truecrypt.htm. Scroll about halfway down the page until you see *TrueCrypt Setup 7.1a.exe* (or *TrueCrypt 7.1a Mac OS X.dmg* if you're on a Mac). Click that link, and once the file has finished downloading, double-click it to install it. Installation is very simple, just follow all the prompts you are shown. Once the program has finished installing, go ahead and run it.



From the main TrueCrypt window, click the **Create Volume** button to launch the Volume Creation Wizard.

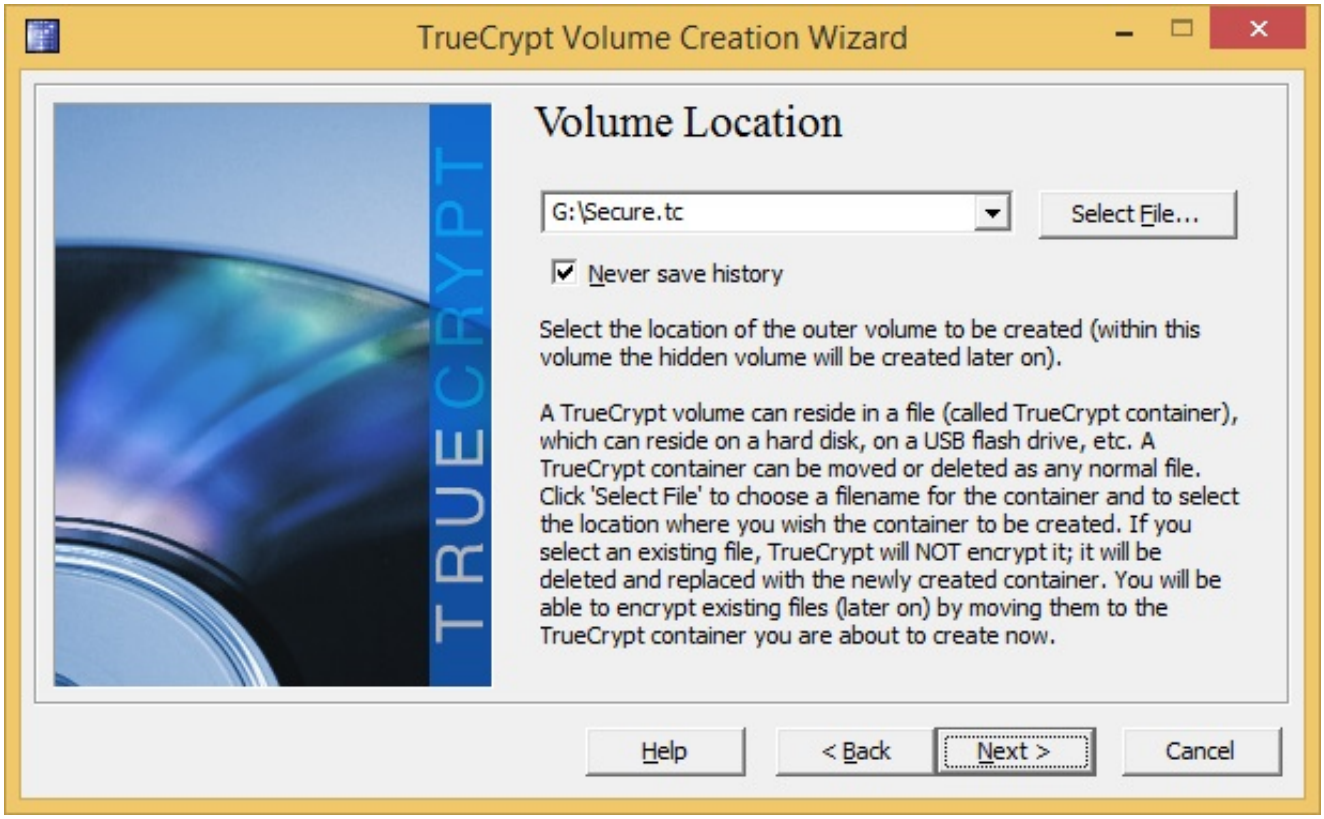


Click **Create an encrypted file container**, then click the **Next** button.



On the Volume Type page, click **Hidden TrueCrypt volume**, and then click**Next**.

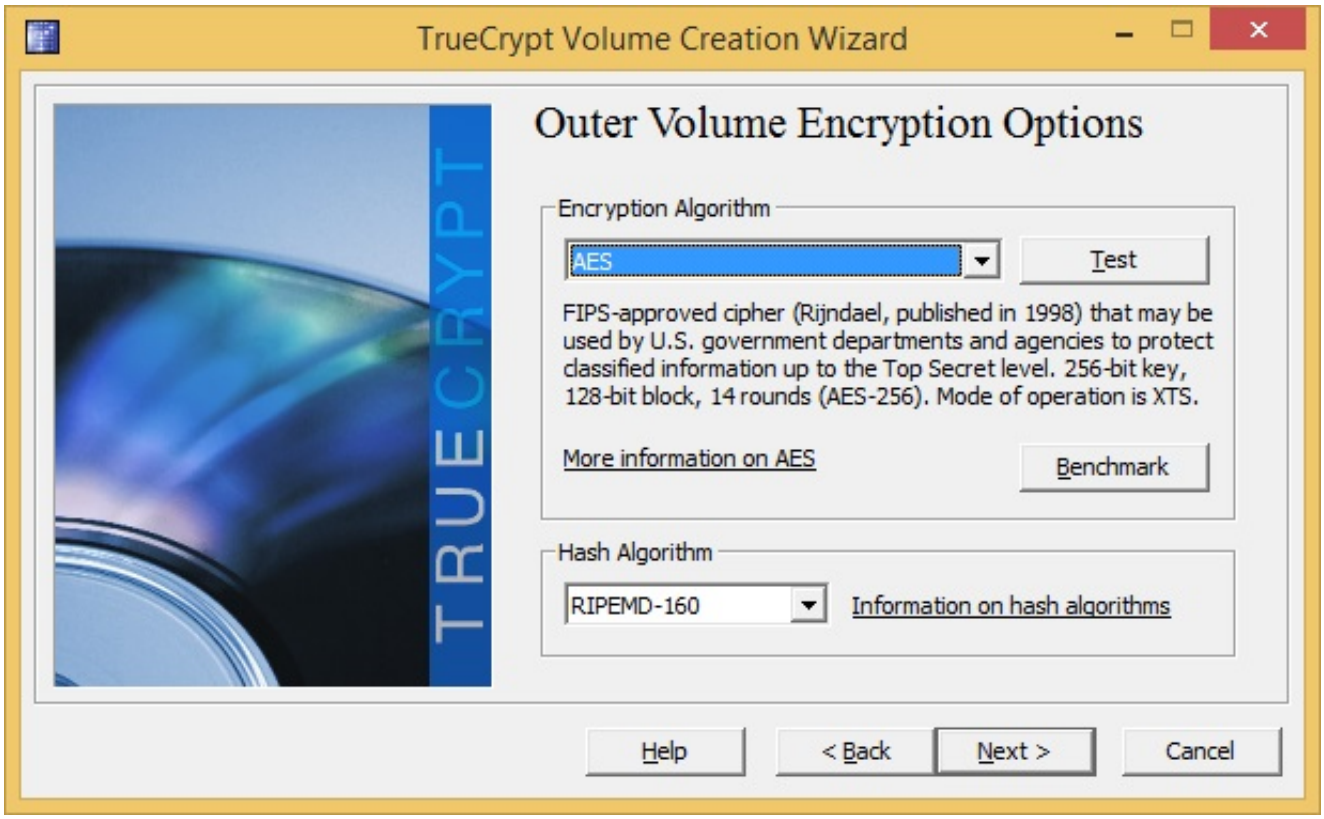
On the Volume Creation Mode page, click **Normal mode**, and then click **Next**.



Next you need to tell TrueCrypt what you are going to encrypt. TrueCrypt creates a single file on your thumb drive that is encrypted; this is the container that will hold all of your protected files. You just need to type in the drive letter and the filename you want to create (the name can be anything). In the example above, my thumb drive is the

G drive, so I typed G:\Secure.tc. Click the **Next** button.

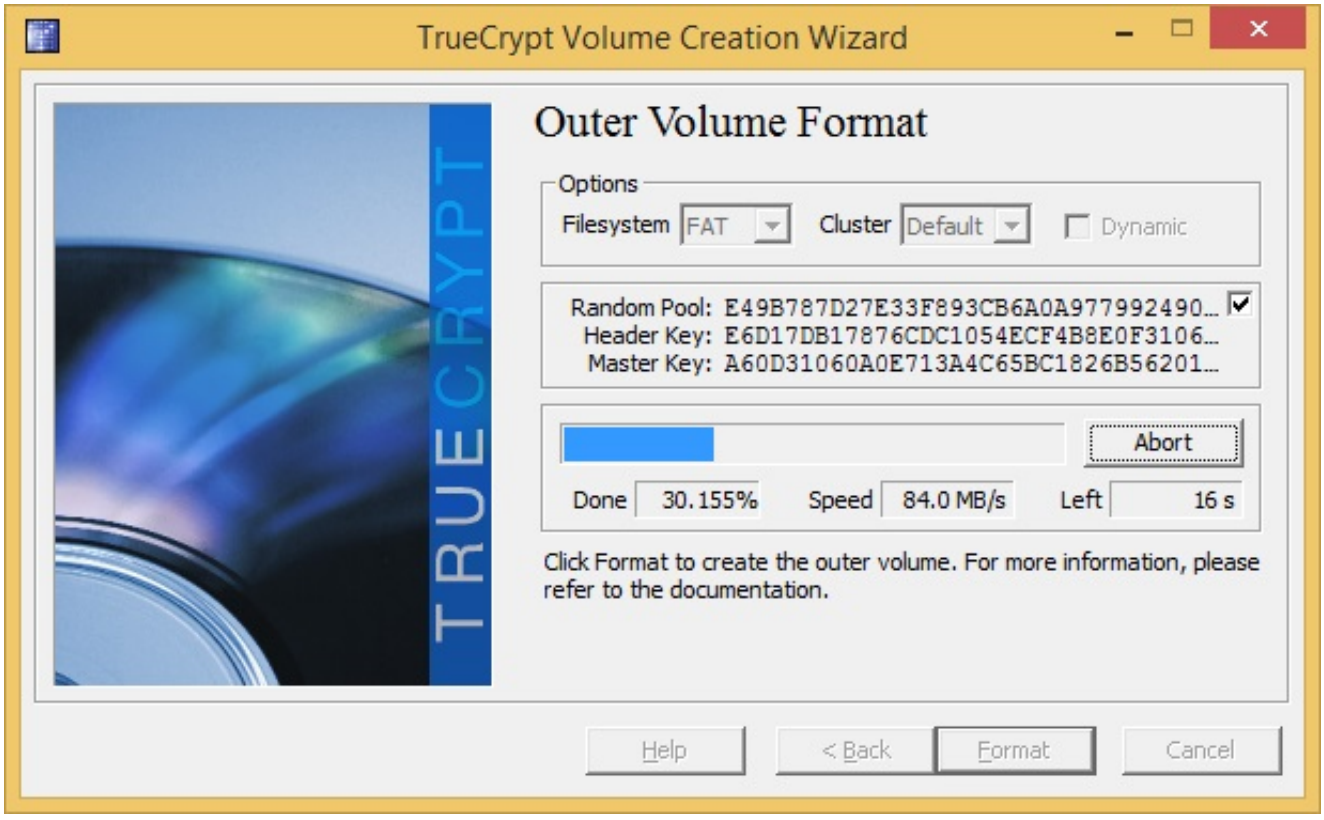
The next page tells you that you will be setting the options for the outer volume. This is the "main" container, the one that you can give out the password as a decoy. Just click **Next** here.



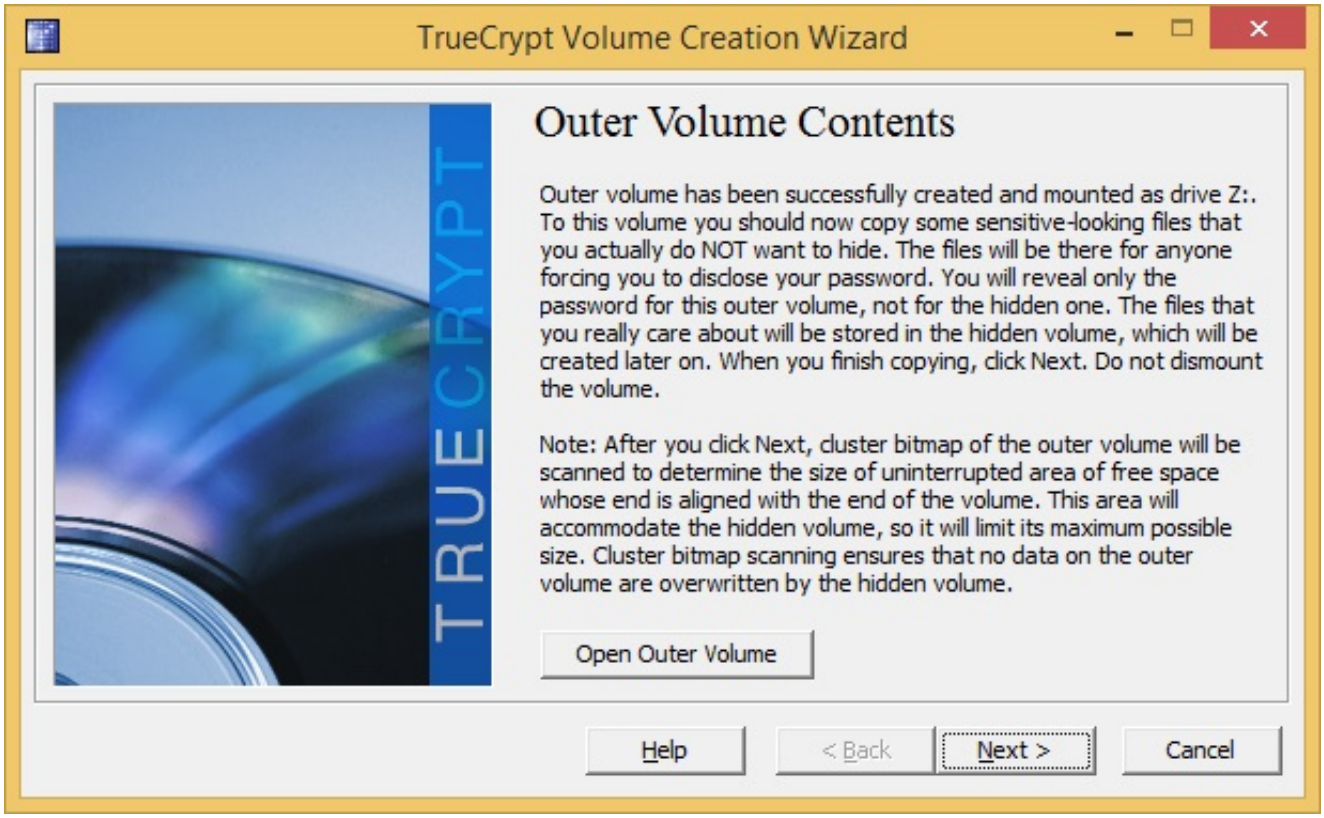
The next page, Outer Volume Encryption Options, let's you choose what type of encryption you are going to use. There are many choices, but they're all very solid, you really can't go wrong with whatever you pick. I usually just leave it at the default selections and click **Next**.

On the next page, Outer Volume Size, you'll set the size of the container you're going to create. You'll have to decide whether you want the encrypted container to take up the entire thumb drive, or do you want to leave some unprotected space where you can store files and not need a password to open them? Also, you'll need to leave some space free to copy TrueCrypt files onto the thumb drive. I want to use my entire drive for protected files, and I'll leave 10 MB of space free. You can see above that I have 1.96 GB free, but the box won't let me type in 1.95 - I can't use a decimal point. So I typed it in as MB instead - since 1 GB = 1000 MB, that means I have 1,960 MB free, so I typed in 1950. Click **Next**.

Next, on the Volume Password page, you'll create a password for the "main" container. Remember, you'll be creating two passwords today. Do you see the image above, and how short the password is? That's a bad idea - you should create a longer password. You might create a passphrase rather than just a simple password - something like *MyBeautifulWifeIsAwesome!* (with the exclamation point included...), that's much better than something like *mypassword1*. Click the **Next** button.



On the next page, Outer Volume Format, you'll need to move your mouse around for a bit to generate some random numbers. Once you've wiggled the mouse for about a minute or so, click **Format**. Depending on the size of your thumb drive, the formatting process could take a while, so just sit back and be patient.



Eventually the formatting will be complete and you'll be taken to the page shown above. At this point, you can copy your files that you don't really care whether they stay hidden or not - your aunt's cookie recipe, some old love letters, the first draft of your novel, etc. Click **Open Outer Volume** and copy those files in there, then close that window (the one that just opened, not the TrueCrypt page) and click **Next**.

Now you'll create the hidden container. The steps are basically identical, so I'm not going to include the screenshots that are the same.

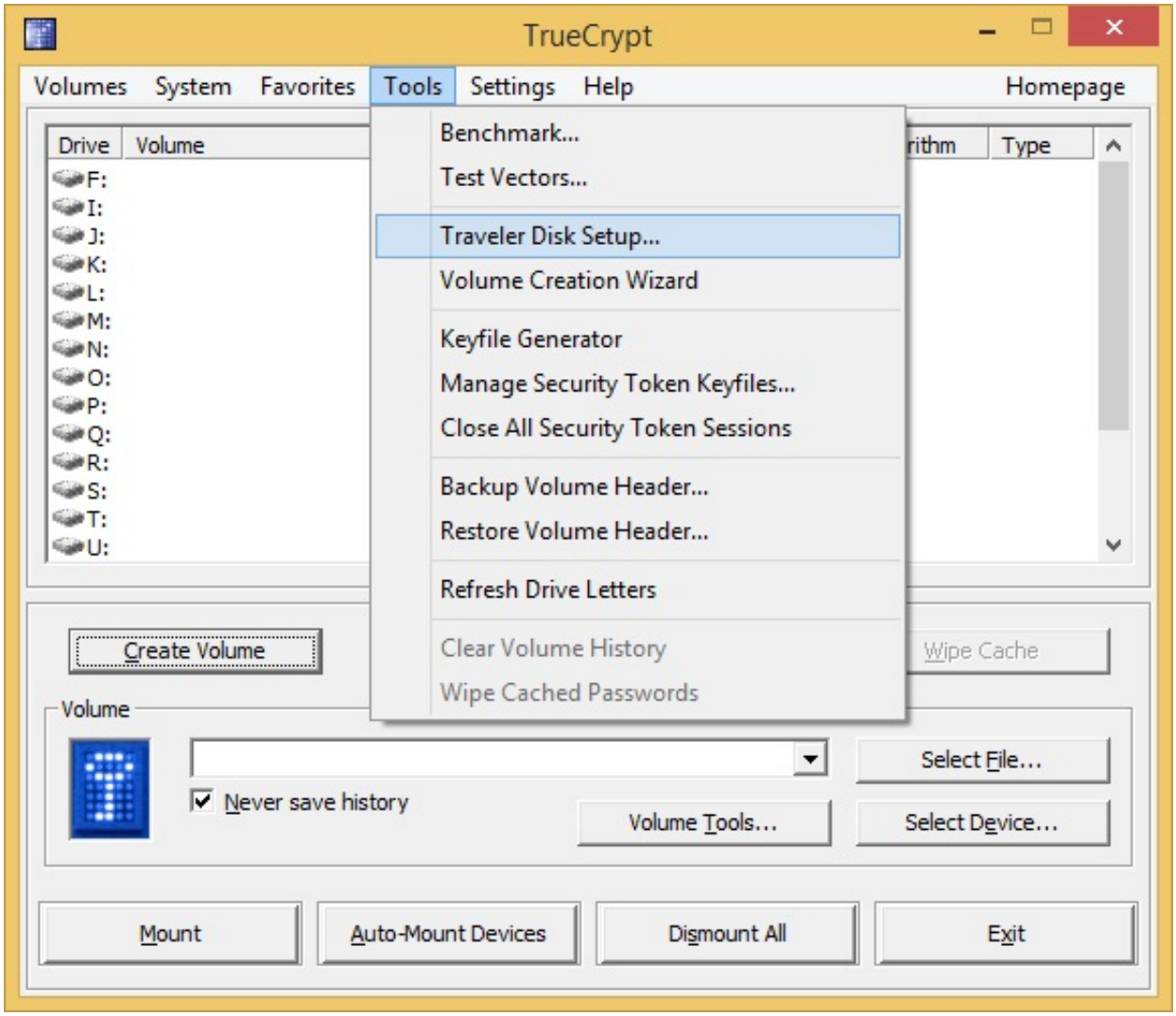
First you'll be asked to choose the encryption options, you can just click**Next**.

Next you'll set the size of the hidden volume. The hidden volume is being created inside the volume that was just created, so in theory you could have it use the maximum amount of space available. However, if you think you might ever want to add some more files to the "decoy" container, then you want to make sure you're hidden volume isn't using up every available bit of space. If it does, and you wind up adding more files to the decoy container later, you could end up deleting some files from your hidden container. For this reason I always put all of my decoy files in at once, set the hidden volume to the maximum size, and never add any more decoy files.

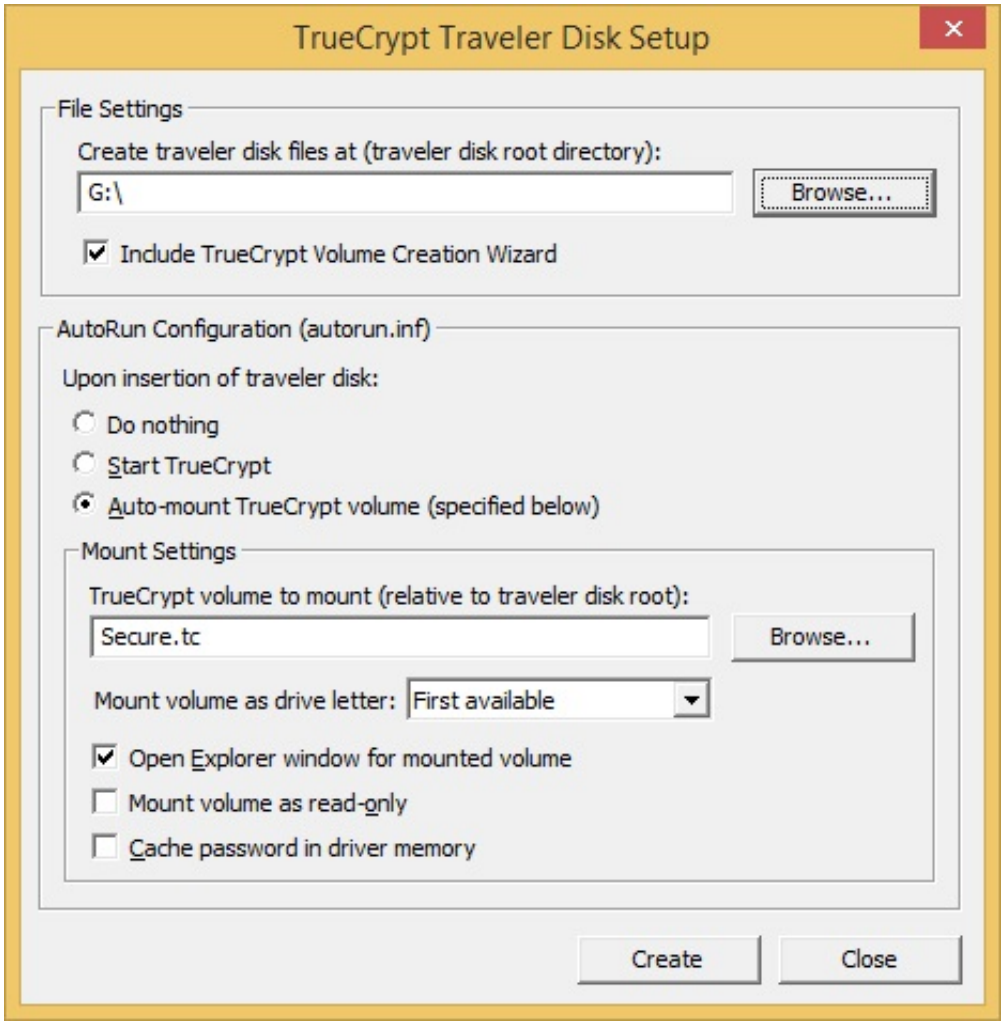
On the next screen you'll create a password for the hidden volume, and then after that you'll format it. Again, this may take a few minutes, so just be patient.

Once the hidden volume has been created, you'll see the page above. You're not going to be creating any other volumes, so just click **Exit**.

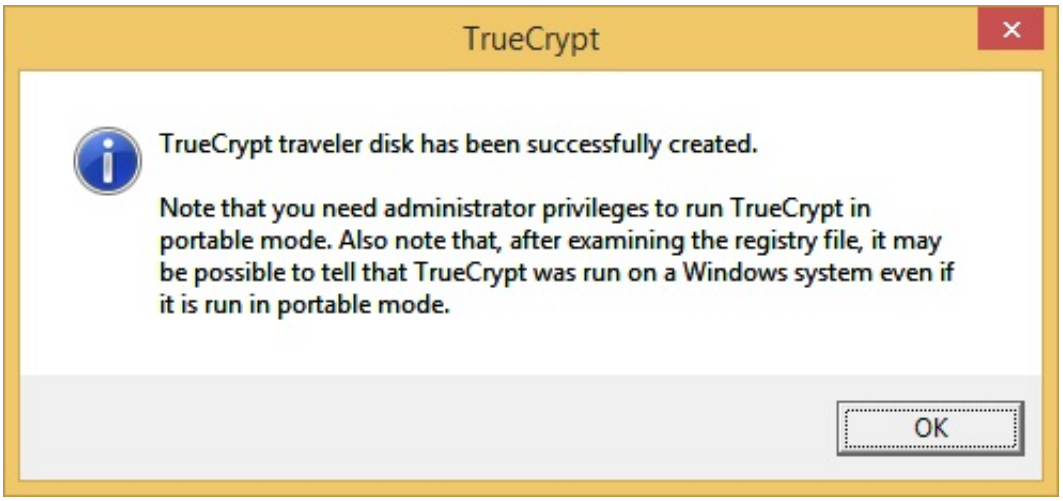
At this point your hidden container has been created, but you need a way to open up the containers on a computer that doesn't have the TrueCrypt software loaded. Fortunately, TrueCrypt has a function that makes this easy.



Back in the main TrueCrypt window, click the **Tools** menu, then click**Traveler Disk Setup**.



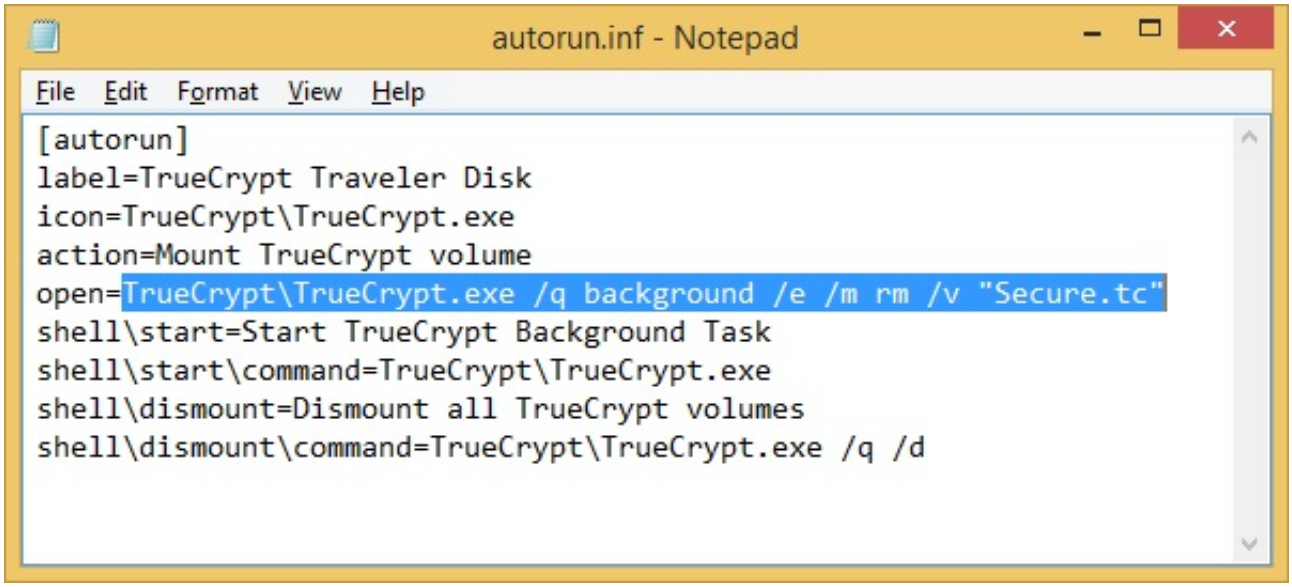
On the next page, you'll enter the drive letter of your thumb drive (mine was G:, yours will probably be different), and name of the file (the container) that you created earlier (in my case, Secure.tc), and click **Create**.



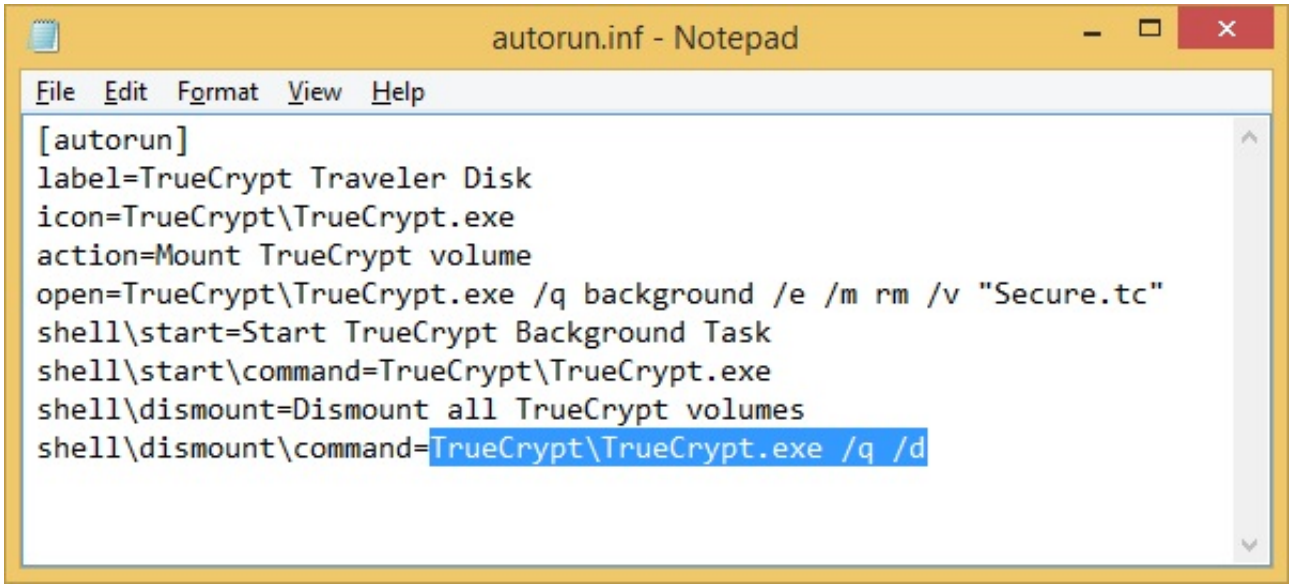
When the files have been copied over to your thumb drive, you'll see the message shown above. This is important to remember - in order to open your encrypted files, you'll need to have administrative rights on the computer you're using. This shouldn't be a problem if you're using your own computer, or even a friend's, but you could run into

trouble if you try to use something like a computer in a library that is heavily locked-down.

At this point, if you look at the contents of your thumb drive, you should see three files - the encrypted file you created, a TrueCrypt folder, and a file called autorun.inf. This last file is intended to run automatically whenever you plug the thumb drive in, and it would launch TrueCrypt and ask you for your password. However, most Windows computers have the AutoRun function turned off (it's a security hazard), so the program will never run. Instead, we'll create two files to open and close your encrypted file.



Using Notepad, open the autorun.inf file and copy all of the text after **open=**(as shown above). Open up a new file in Notepad, paste that text into it, and save the file to your thumb drive as **LoadSecureFile.bat**.



Open up autorun.inf again, and copy all of the text after shell\dismount\command= (as shown above). Open up another new file in Notepad, paste that text into it, and save the file to your thumb drive as**UnloadSecureFile.bat**.

Once both of these files have been created on your thumb drive, you should be able to plug the drive into any computer (as long as you have administrative rights...), double click the LoadSecureFile.bat file, and TrueCrypt will ask for your password. If you enter the password you created for your "main" container, you'll see the files that you copied over earlier, and nothing else. There's no indication that there's anything else on the disk. Close that window, and double-click UnloadSecureFile.bat. Your files are now protected again. Double-click LoadSecureFile.bat again, enter the password for your hidden container, and you'll see an empty window, ready to save all your super-secret files - your Hydra membership card, Powerpoint presentation for taking over the world, etc.

One thing to keep in mind - once you enter your password and can see your secret files, you are at the mercy of the machine you are using. If the owner has installed anything to capture the keys you type, he'll have your password. There could even be software installed that would automatically copy all your files without you seeing anything. So be sure you trust where you're accessing your files.

What To Put On Your Secure Drive

Now that you've got your secure thumb drive set up, what should you put on it? Basically, anything you have written down that you might need to contact someone else, access your financial information, get medical help, and prove who you are. I recommend:

- Identification Cards - driver's licenses, school and military ID, social security cards, passports, concealed carry permits
- Medical Information - insurance cards, shot records, prescription lists
- Financial Documents - list of bank and investment account, usernames and passwords, copies of your credit and debit cards
- Family Records - birth certificates, marriage licenses, divorce decrees, adoption paperwork, wills
- Property Records - home and vehicle titles
- Photographs - both current pictures, and irreplaceable photos

Protecting Your Secure Drive From EMP

If you have a rugged thumb drive, then you're protected against water, heat, and drops, but what about EMP? There's no completely foolproof way to protect your drive from an EMP and still keep it portable--after all, there's no way to test your protection method ahead of time, so short of storing it in an underground vault you just have to hope for the best. But there's an easy way to make a case that should (hopefully) get you through it.

I've said before that I love Altoids tins, and here's another use for one. Place the thumb drive inside a ziploc bag, then wrap the bag with a layer of foil (you can cut the bag down to size to avoid it being extremely thick, you just want a layer of plastic between the drive and the foil). Then place the wrapped drive into another ziploc, and wrap it with foil again. Place it into one more bag, then inside the Altoids tin. So, from the inside out, you've got thumb drive, ziploc, foil, ziploc, foil, ziploc, Altoids tin.

Obviously, if an EMP were to occur, you'll have to figure out a way to actually access the data on your secure drive, but hopefully computers can eventually be restored--lost data can't!

I know this was a lot of steps to get a secure hiding place for your documents set up, so if you have any questions or run into any problems, please let me know in the comments!

Bill Osuch

Contributor at Self Reliant School

Bill has been prepping and urban homesteading for over 10 years. He is the father of 3 active, inquisitive boys who have followed him into geekdom. When he is not working on a project with his boys, he enjoys reading, traveling and target sports.

Spread The Word

You Might Also Like:

EMP: What You Need To Know To

Pandemic: What you need to know

Can You Buy Guns Through The Mail?

7 Ways To Start A Part-Time Business

6 Simple Auto Maintenance Jobs

5 COMMENTS FILED UNDER: GENERAL PREPPING TAGGED WITH:ELECTRONIC SECURITY, EMP, FARADAY

COMMENTS

doug says
April 23, 2015 at 2:28 pm

thanks Bill for this thought and effort!
doug

Reply

pam says
April 23, 2015 at 7:37 pm

Well, that's really nice…IF you work on a PC. And for Mac users…?

Reply

Bill Osuch says
April 23, 2015 at 8:06 pm

As I said in the article above, if you're on a Mac you would download the file *TrueCrypt 7.1a Mac OS X.dmg*. Other than the drive letters, the process is identical.

Reply

Debrah Nadler says
April 24, 2015 at 8:39 am

Very thorough and informative. Thanks

Reply

Illini Warrior says
April 24, 2015 at 11:40 am

In regard to a flashdrive protective container for everything including EMP …. an all metal "match safe" is a great solution …. the perfect container for portability in the lap top case, brief case, BOB/GHB or even a pocket EDC item ….

Reply