Encrypting Folders and Files on Windows

Creating Encrypted Containers with VeraCrypt

(for simple file-based encryption - check the help files for a particular software product – many, such as Microsoft Office and Adobe Acrobat, have built-in tools to encrypt (password-protect) documents.

VeraCrypt is a cross-platform encryption tool that allows you to create 'containers' on your local hard drive. This allows you to create a password-protected container file that will mount as a "drive letter" in Windows Explorer only after a decryption key is entered -- without the decryption key, the data is unreadable by anyone who merely has access to the file. Think of this "file" as a password protected folder that only opens when properly unlocked.

The following instructions will walk you through basic setup on a Windows 10 computer.

(If you are on a Macintosh -- there are native tools built into the OS that achieve the same goal – see our Macintosh page here.)

If you are interested in a full-disk encryption solution with your Whitman-owned/managed device -- please contact the WCTS Help Desk or the Information Security Office for a discussion about the options available to you.

For personal machines – you are encouraged to seek out Microsoft's documentation on using Bitlocker drive encryption.

**** Reminder: modern encryption tools are very powerful. If you lose or forget your decryption key (password) -- the encrypted data is effectively lost. Proceed with caution and understand the potential data loss risks.**

Before proceeding you will need to install the VeraCrypt software:

1. Download VeraCrypt directly from the project home page
   <https://www.veracrypt.fr/en/Downloads.html>
   or from Sourceforge
   <https://sourceforge.net/projects/veracrypt/> and follow the install instructions.
2. Launch VeraCrypt

Step-by-step guide

To create a new protected container:

1. Select **Create Volume** from the main application window.
2. Select **Create an encrypted file container**
3. Click **Next**
4. Select **Standard VeraCrypt** volume
5. Click **Next**
6. Click **Select File…** in the Volume Location window
7. Type in your desired filename and select the location in the file browser
   (it is recommended to use a .hc file extension)
8. Click **Save**
9. Click **Next**
10. Choose Encryption and Hash Algorithms (defaults are fine)
11. Click **Next**
12. Choose container size
13. Click **Next**
14. Enter and confirm password for the container
15. Click **Next**
16. Move the mouse around inside the Volume Format window to aid in creating complex, random cryptographic keys.
17. Click **Format** when you feel your key is sufficiently random
18. Click **Exit** in the Volume Created window

To mount and use your encrypted container:

1. Double-click on the .hc file in Windows Explorer
   (or launch VeraCrypt and open from there)
2. Select a drive letter
3. Click the **Mount** button
4. Enter the container password
5. The container will now show up as the previously-chosen Windows drive letter.
6. The container will automatically dismount upon logoff.

You can now copy, move, or create data in this location. It is recommended that any sensitive data be stored in this encrypted location so the files are only 'unlocked' when the data is needed -- this adds an additional level of protection should someone gain access to your hard drive.

To disconnect the container/drive letter without logging out:

1. Open the VeraCrypt application
2. Select the drive letter you wish to dismount
3. Click Dismount

Encrypted file containers can be moved and used on multiple computers provided both computers have VeraCrypt installed.

Related articles

- Creating a Secure Password
- Multi-Factor FAQ
- Encryption
- Encrypting Folders and Files on Mac
- Encrypting Folders and Files on Windows