

# ENCRYPT YOUR IMPORTANT FILES TO HIDE THEM FROM VIEW

Chances are, there are files on your computer that you don't want other people (including cybercriminals) to see, whether it's banking data, your investment accounts, medical expense records, email correspondence, or other documents.

A highly-rated program called **AxCrypt** makes it easy to encrypt (code) all types of files, ensuring that all your sensitive data are safe from prying eyes.

The program integrates easily into Windows, appearing as an item in any file's context (right-click) menu. You can simply right-click on the item you want to encrypt, select AxCrypt from the menu, and choose Encrypt. The program lets you select a password for the file and optionally create a key-file. As its name would suggest, the key-file is designed to function as a key that can unlock encrypted files. It's meant to be kept on a removable storage device, such as a USB drive, so that it can only be used when the you insert the removable device into the computer with the encrypted file. In addition to encrypting the original file, the program also lets you encrypt a copy, encrypt a copy to .EXE, and shred and delete files. The program has a Help file in the form of an online PDF, and it's quite thorough with plenty of screenshots. Overall, both evaluators and users have judged AxCrypt to be both powerful and easy to use and a great way to keep files secure for users of all experience levels. AxCrypt installs politely and uninstalls without issues.

1. Go to this [link](#) to download the FREE program.
2. Follow the setup instructions and after it has completed, exit out of the setup wizard.
3. Create a folder for all the files that you want to encrypt. You can place this folder in any convenient place, whether it's on your desktop in full view or partially hidden in Windows Explorer.
4. Once you have created the folder, then move your target folders and files into the folder.
5. Right click on the folder and scroll down to **AxCrypt**. Next, select **Encrypt** and a box will prompt you to enter and confirm a password.
6. Open your folder and you'll notice that the icons have changed. Double click on one of the files and you will be asked for your password. The file will only open if the password is entered.
7. While using a password to secure your files is a good idea, a key-file is even more secure. A key-file is a special text file containing a random string of characters,

which is your key. The file is placed on a USB drive, which means the encrypted folder can only be opened if the USB drive is plugged in and AxCrypt is pointed to the correct key-file. If that sounds a little too complicated, don't worry! It will all make sense once you're finished.

8. Go ahead and plug in your flash drive. Right click on your encrypted folder, click **AxCrypt**, then **Make Key-File**.
9. Find the directory for your USB drive and click **Save**. Open the **Encrypt** dialogue box again and enter your password twice. Also, where it says **Key-File**, choose the one you just saved on your USB drive and click **OK**.
10. Now, when you try to open a file in the encrypted folder, you will be prompted to select the key-file. Someone who doesn't have access to your USB drive will not be able to open the files, even if they know your password.
11. It's good to know that all of your private documents can only be accessed if the USB drive is present. It's very important for you to never accidentally delete the key-file. It's actually a good idea to make a copy of it and keep it on another disk somewhere safe.
12. There is another feature of AxCrypt that provides even more security. If you want to delete files that contain sensitive information, AxCrypt contains a shredding feature that overwrites the deleted files with random information. If you want to "shred" a file, right click on it, choose **AxCrypt** and then select **Shred and Delete**.