Encrypting a file before sharing

Encrypting a file before sharing

Context

This article is useful for those who want to share an electronic file that contains sensitive information.

Note that if you have whole disk encryption on your computer, the files on it are not encrypted, only the drive on which the files reside. So if you send a file to someone via email or other means, the file itself is not encrypted.

File encryption is different from whole disk encryption. It allows you to put a password on a file or a folder. The recipient needs the key (password) to decrypt the contents of the file/folder.

Using cloud storage, such as Dropbox, that has encryption built in, might seem like a good idea. However, most cloud storage companies also hold the decryption keys, meaning they could decrypt your files should they need to. If you do use the cloud, make sure you add encryption to sensitive files in addition to the encryption already in place.

Warnings

⚠ **Not all encryption methods are created equal!** Make sure you are using a file encryption tool that encrypts according to DoD (Department of Defense) standards, which is the AES (Advanced Encryption Standard). It supersedes DES (Data Encryption Standard).

⚠ **Safely store the password to decrypt!** If you lose your password, you will NOT be able to decrypt the contents of the file(s). Lastpass Password Manager is one option to save your passwords securely.

⚠ **Use a strong password!** If the password is easy to guess or crack, then the contents it is protecting will not be secure, even if encrypted.

Answer

Below are some of the most common tools that can be used for file or folder encryption. **These tools are not licensed by IS&T**, and the IS&T Service Desk may not be able to assist you with troubleshooting. You can still contact the vendor directly for support.

VeraCrypt (Windows, Mac, Linux, Free)

A popular free open source disk encryption software for Windows, Mac OSX and Linux by IDRIX. Amongst its many features, it can encrypt an entire partition or storage device such as USB flash drive or hard drive. It's real-time encryption allows data to be read and written as fast as if the drive was not encrypted making the end user experience completely transparent.

Cryptomator (Windows, Mac, Linux, Free - Pay what you want)

Cryptomator provides transparent, client-side encryption for your cloud (but can also be used in non-cloud situations). Cryptomator is free and open source software, which encrypts file contents and names using AES. Your passphrase is protected against bruteforcing attempts using scrypt. Directory structures get obfuscated. The only thing which cannot be encrypted without breaking your cloud synchronization is the modification date of your files.

Instructions on installing Cryptomator and creating encrypted volumes can be found at Cryptomator for Cloud-Sharable Encrypted Volumes.

GNU Privacy Guard (Windows, Mac, Linux, Free)

GNU Privacy Guard (GnuPG) is an open-source implementation of the famed Pretty Good Privacy (PGP) encryption tool---you can read the very interesting history of PGP and how GnuPG came to be here. GnuPG is a volume and individual file encryption tool with support for a dozen

encryption schemes, paired keys, and expiring signatures. GnuPG doesn't only provide rock-solid local file encryption; it is, thanks to paired encryption and public key servers, a great tool for encrypted communication. Please note, regular old GnuPG is a command line tool. Check out the list of graphical wrappers and application plug-ins for various operating systems here.

Disk Utility (Mac, Free)

Disk Utility is a diverse tool that handles almost any disk-related tasks you'd need on OS X. The utility is capable of creating secure disk images and file volumes encrypted with AES 128-bit or 256-bit encryption. Like most native Mac utilities and applications, Disk Utility and the accompanying encryption blends seamlessly into the OS X experience and makes mounting and un-mounting encrypted volumes a breeze. Instructions by Apple.

7-zip (Windows, Free)

Compared to some of the heavyweights, like GnuPG and TrueCrypt (no longer available!), it might be easy to dismiss the popular file compression tool 7-zip as a lightweight. 7-zip fills a perfect niche for many people, however, by offering simple ZIP container-based encryption. If you're not interested in encrypting a ton of files or maintaining an entire encrypted volume, but you still want to make sure important documents like tax returns or other Social Security bearing documents are locked up tight, 7-zip sports strong AES-256 encryption. Create a new compressed archive, throw your files in it, and slap a password on. Your files are strongly encrypted and stored right alongside your regular documents.

AxCrypt (Windows, Free)

AxCrypt is a free encryption tool for Windows. Once installed it integrates with the Windows shell and offers simple right-click encryption and decryption of files with AES-256 encryption. Your entire interaction with AxCrypt can take place exclusively from the right-click context menu. In addition to integrating with Windows and offering easy encryption and decryption, you can also use the tool to create self-extracting archives to securely transport files or transfer them to a friend---no AxCrypt installation necessary at the other end.

PGP Zip (Windows, Free with PGP Desktop)

If you have PGP Desktop installed on your machine, you can use a tool that comes included with the software, called PGP Zip. Instructions on how to use PGP Zip, supplied by Symantec.

> **TrueCrypt Alternatives**
> TrueCrypt is no longer being maintained by SourceForge and is not a secure option for file encryption. Here are some alternatives.

See Also

- Encryption Landing Page