Encrypt Your Documents

Don't Let Your Private Data Fall Into The Wrong Hands

Imagine that you're having lunch at the airport while you wait for your plane to arrive and take you on a family vacation. To pass the time, you use your notebook to send a few emails and check the weather in your destination city. You suddenly notice that it's time to make your way to the gate, and in your excitement, you accidentally leave your notebook behind. By the time you realize that your notebook bag is empty and return to the food court, your notebook is gone.

Think about the types of information you have stored on your computer's hard drive. Do you have family photos and videos? Your favorite music albums? What about financial information, passwords, and other sensitive data? Encrypting vulnerable information protects it in the event that your computer is lost or stolen.

We'll show you some of the most common ways to safeguard your digital documents and offer additional tips for protecting your private information.

Password-Protect Documents

Whether you're using Microsoft Office to organize financial numbers or write a private journal, you likely want to keep your personal information safe from prying eyes. One way to block unauthorized access to your documents is to simply add a password that must be entered before the document will open. But even though adding a password to your documents is a good way to deter someone who sits at your computer desk and attempts to read your files, it is not as strong as other encryption methods. Some programs are made specifically to crack Office passwords, so if your computer is stolen, your data may still be at risk. Keep in mind that using an Office password is just one of many encryption methods that you should use.

Password-protecting your Excel or Word document is simple. First, create a new document or open an existing project. In Word 2007, click the Office button and choose Save As. In the Save As dialog box, click Tools on the bottom left and then select General Options. Under the File Encryption Options For This Document section, locate the text field next to Password To Open. Type your preferred password in the field.

You can also add a password that must be entered in order to make changes to the document. Under the section File Sharing Options For This Document, type your preferred password in the text field next to Password To Modify. Click OK. Upon exit, you will be prompted to re-enter the Open and Modify passwords to ensure correct spelling. Once completed, continue to save your document as you normally would.

The next time you open your Word document, you will be asked to enter your password before the document will open, which helps prevent information leakage should an unauthorized user get ahold of your computer.

Encrypt Your Hard Drive

Password-protecting your most sensitive documents is a good start. But what if some programs don't offer a password option? Windows BitLocker Drive Encryption, included in the Ultimate editions of Windows Vista and Windows 7, can be used to encrypt your entire hard drive. With BitLocker, every time you save a file to your hard drive, it is encrypted automatically. Encrypting a file means that the contents of the file are scrambled so that only someone with an encryption key can unscramble and read the file.

BitLocker ensures that every file on your hard drive is protected from unauthorized viewing, even if your computer is lost or stolen or if the hard drive is removed and installed in a different computer.

You can access BitLocker in the Security section of the Control Panel. In order to run BitLocker, however, your computer must first have a supporting OS (operating system) and a TPM (Trusted Platform Module), which is a piece of hardware built into your computer's motherboard.

Safeguard Your Files

If you're unable to use BitLocker to secure the data on your hard drive, you can use a third-party encryption product instead. For example, PGP offers several encryption products, such as PGP Desktop Home ($99; www.pgp.com). The software can encrypt individual files, email messages, and instant messages from some services by

creating a virtual disk on your hard drive that works much like a removable drive. To see if your email or instant messaging client is supported, visit PGP's Web site.

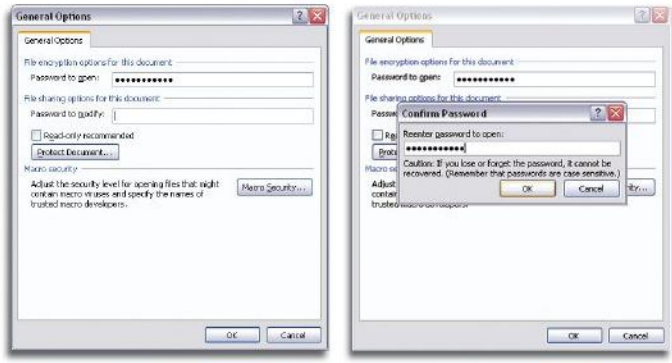
Dropping a file into the PGP Virtual Disk Volume automatically encrypts the contents of that file, and the virtual disk volume is the perfect place to store financial, banking, or other sensitive information.

Another encryption option is TrueCrypt, which is free to download and works much like PGP's Desktop Home in that it creates a virtual encrypted disk where you can store personal files. TrueCrypt also encrypts whole storage devices, such as USB flash drives or external hard drives. To download TrueCrypt, navigate to www.truecrypt.org and click Downloads at the top of the page. Click Download under the Windows 7/Vista/XP/2000 section and save the file to your hard drive. Once the file finishes downloading, double-click the executable and follow the installation instructions.

When turned on, Windows BitLocker Drive Encryption automatically encrypts all files saved to the hard drive. BitLocker is available in the Ultimate editions of Vista/Win7.

Encrypt Your USB Flash Drive

Ideal for people who are always on the go, a password-protected USB flash drive, such as the 2GB IronKey Personal S200 ($99; www.ironkey.com), encrypts every file that's saved on it. In addition to file encryption, IronKey provides private Web browsing that you can use whenever you are using a public computer and secure password management, so you can keep a list of all the passwords you use on the Web.



You can prevent unauthorized users from viewing your Microsoft Word documents by adding a password that must be entered before the file will open. After you've designated a password for your document, Word will prompt you to re-enter the password to ensure it is spelled correctly.

Create A Strong Password

Whether you're password-protecting an Office document, your Windows user account, or a USB flash drive, the password you choose has to be a good one; otherwise, a malicious user could decipher it easily with a few tools. Following are several tips for creating a strong password.

First, we recommend that a good password be at least eight characters long, though, Microsoft suggests that your passwords should contain at least 14 characters. Ideally, these characters should be a combination of uppercase and lowercase letters, numbers, and symbols. It may seem like a difficult task creating (and remembering) a seemingly random collection of characters, but you can use the accompanying chart to learn a simple way to create a complex password.

Other password tips include avoiding words from the dictionary; sequences, such as 1234; or repeating characters. Lastly, avoid using personal information, such as your name, phone number, or birthday.

Safety First

We all have data on our computers that we'd like to keep private, especially if it could pose a financial or identity risk. Being aware that a password may be needed to protect sensitive data is the first step to safety, and by implementing one or more of the suggested encryption methods above, you can ensure that none of your personal data falls into the wrong hands. ❚❚

BY KRIS GLASER BRAMBILA

Creating Passwords

Use the suggestions in this chart to create a strong password.

Password Building Steps	Example
Start with a passphrase	My favorite food to eat at lunch is pizza.
Shorten the passphrase to the first letter of each word	mfftealip
Capitalize several of the letters	mfFteAliP
Add your age between two of the letters	mfFteAli24P
Increase length by adding punctuation and/or symbols	[mfFteAli24P!]