

“Disaster-proof your documents.”

Plan ahead for an emergency by digitizing your essential personal info.

By Kevin Savetz

© Computer Shopper, June 2006

Step 1: Gather your originals

If you had to evacuate due to a storm, a fire, or some other emergency, what documents and information would you want with you? Your first task: Think this over, then gather all of your important files. Depending on how organized you are, this could be the most time-consuming part of the project.

You'll likely need to track down your insurance information, bank-account numbers, and other financial records. The best way to digitize these items, however, depends on the kind of info in question. For instance, you can store a list of your credit-card and bank-account numbers, along with the banks' phone numbers, in a text file. For medical records, birth certificates, insurance policies, and Social Security cards, however, scanning in these items is your best bet.

Step 2: Scan your paper records

Now that you've gathered your originals, you'll need a PC and a scanner to digitize them. Scanning the documents in gray scale should suffice. (Preserving color isn't important, and gray-scale scanning is usually faster.) Remember to scan both sides of the documents, if necessary, and use a reasonably high resolution. We recommend at least 300 dots per inch (dpi)—that way, you'll be able to print clear copies should the need arise. Be sure to save the images as JPEG files or in another common format viewable on any computer without special software.

As you scan and save the documents, organize the files into directories that best describe the contents. For instance, label them "life insurance policy" or "Kevin's medical records."

TIP

If you don't want to invest in a scanner, drop by your local FedEx Kinko's to scan your documents. Self-service scanning costs 35 cents per minute.

Step 3: Take inventory of your possessions

Many insurance companies advise customers to create an inventory list of everything they own, where they purchased the items, and how much they paid. Being able to prove that you own an expensive piece of art or a high-end PC could mean a hefty difference in the size of your insurance claim, but creating a detailed inventory usually seems like an insurmountable chore.

It doesn't have to be, however. Simply walk around your home with a digital camera or video camera to capture your possessions. This should include artwork, jewelry, expensive electronics, and other costly items. If you have the receipts handy, scan them,

or take clear, close-up photographs. Save the digital images with your other important files.

Step 4: Store it and back it up

Now that you've collected and digitized your vital information, you'll need to store it where you'll be able to find it quickly and easily. That means archiving the information somewhere other than on your PC.

Because you want the data to be readily accessible when you need it, don't use any type of media that isn't universal to all computers. One option is burning the files to CD or DVD. The long-term viability of disc media—especially less-expensive, lower-quality brands—has been the subject of much debate, so it's a good idea to make two or three copies of each disc, using different brands of media.

Better yet, store the data on a USB flash drive. You can easily dedicate a 128MB thumb drive to this purpose for as little as \$10. Plus, it's easy to grab and tote in an emergency.

Now's also a great time to burn a few more important discs: one with your digital photo library—you know, the family-vacation photos you'd hate to lose if your hard drive crashed—and one with the other important files on your PC, such as your business and tax records, e-mail address book, and important correspondence. Again, backing up these items onto a USB flash drive will make them easy to grab when needed. The goal isn't to create a complete system backup, but to make an archive of your most-important files.

Of course, you should store your data somewhere that's secure, such as a safe-deposit box or fireproof safe, and let your loved ones know how to access it in the event that you can't. You could make the argument for encrypting these important, sensitive files, but encryption could cause problems if you or another family member must retrieve the data but don't have access to the password. As long as your media is stored in a secure location, encryption shouldn't be necessary.

If you insist on encryption, however, several free or inexpensive tools are available. [TrueCrypt](#) is a free, open-source program for Windows and Linux that can encrypt an entire folder or drive (such as a USB key) so that it's password-protected. Just be sure to save an unencrypted copy of TrueCrypt with your data so you can decrypt your files later. An alternative is [Steganos Safe 8](#) (\$29.95), which bundles the decryption routines into the encrypted files, eliminating the need for extra software at decryption time.

Step 5: Keep your records up-to-date

An archive of out-of-date documents won't do you or your family any good in an emergency. Make a point of updating your archive annually—more often, if it's feasible. This chore will probably rank alongside doing your taxes or cleaning the fish tank on the excitement meter, but spending an hour or two now can be a lifesaver should a disaster strike.