



Expert View

Six Ways To Store Securely The Keys To Your Online Financial Life

Deborah L. Jacobs, 02.15.11, 6:00 PM ET

No matter how young or hearty you feel, it's important to have a durable power of attorney, appointing a trusted family member, friend or advisor as an agent to act on your behalf in a variety of financial and legal matters if for some reason you can't--say because of mental or physical disability.

But for people who live their financial lives online, a power of attorney alone does not go far enough. Without the keys to your electronic kingdom, your agent can't pay your bills or keep watch on those being automatically charged to a credit card or debited from a bank account. Nor could your agent manage your investments.

These issues, which also arise when someone dies, can be even more troublesome in cases of incapacity, because of the need to meet a person's continuing expenses.

That reality hit home for Karin C. Prangle, an estate-planning lawyer with Krasnow Saunders Cornblath in Chicago, after her father-in-law, then 61, suffered a stroke in 2009. At the time, he had his own home-based business selling building supplies to contractors. Even his wife didn't know that he was using a business credit card to pay vendors and handling all transactions with the card company online.

During the many months that he was out of commission, card statements were piling up in his e-mail; his family didn't have the password to that either. Although he didn't recover enough to keep running the business, he was finally able to tell them about the credit card so they could pay the bills. (The family requested that his name and the name of his company not be included in this story.) But the card company refused to waive hundreds of dollars of interest and penalties that had accumulated.

To save your family from similar hassles, you need to organize your electronic financial records securely and give access to the person you have designated as your agent under the durable power of attorney.

James Lamm, a computer consultant turned trusts and estates lawyer with Gray Plant Mooty in Minneapolis, recommends you start by using a different secure password for each account. Few mortals could come up with enough of these that meet industry standards--at least 10 characters (or more, depending on whom you ask) consisting of a mix of upper and lowercase letters, numbers and symbols. And just to further inconvenience you, for security reasons, a growing number of institutions automatically shut down your access unless you change your password periodically.

If this leaves you flummoxed, you can do as Lamm does and rely on free software or Web-based password generators. Just don't expect to remember the gobbledygook they produce. In fact, if you go this route (and admittedly few people do), you must be extra vigilant about keeping an up-to-date list of your passwords, because you, the hackers and the person who holds your power of attorney will have this much in common: None of you will ever guess them!

Then where should you put this list? The answer depends on your technological fluency and how much you trust online security systems. Remember, too, that you want to make things easy for those who step into your shoes. In a time of crisis (say because of your illness or death), it would be better if your trusted advisors or loved ones didn't need a pricey computer consultant or the 14-year-old next door looking over their shoulder.

Here are some ways to store your passwords, roughly ranging from most to least high-tech. Some of these methods can be combined with each other to create a multilevel locker.

1. Use an electronic password manager. A number of services that function as password generators allow you to enter all your passwords (even those you created yourself) in a single database and lock them up with a master electronic key. You (or your agent) only need to remember one password to access the list. Lamm, who relies on the free service [LastPass](#), likes other features it includes: automatic entry of passwords when you revisit sites, and synchronization across the eight computers that he uses.

In the age of hackers and WikiLeaks, the question of whether you can trust such a system seems debatable--and using one might require a leap of faith. Lamm, who says he's satisfied that the password manager he uses is secure, offers advice for evaluating others. Check that the connection between this system and your device is encrypted. This prevents interception while the data is being transmitted.

Then be sure the data is also encrypted. No one should be able to unlock it without your password, Lamm says. If the company's employees can access it--for example, to monitor for copyright infringement, abuse of their terms of service, or to reset your password--the system is not failsafe. Be aware too that not all encryption is equally secure. The strongest, which is very widely used, is advanced encryption system or AES, he says.

2. Rely on a digital gatekeeper. Several new services, aimed at people who are doing estate planning, charge a monthly or yearly fee to store the digital data that you enter, and release it according to your instructions. One will even check up on you periodically via e-mail, assume you've kicked the bucket if you don't reply, and contact your heirs. Apart from questioning their security, you ought to wonder whether these services will be around when you need them--many are startups. And most are focused on death, rather than incapacity.

3. Put it in a cloud. These are generic online storage services that allow you to store all types of documents, including the list of passwords that you create. To access them, your family or agent would need to know both your password and the name of the document. Your due diligence about the security of these services should be the same as for evaluating any other online service.

If you lead a very mobile life, remote access can be a huge convenience, but here too you must trust the technology. [Bernard A. Krooks](#), a Forbes.com contributor and an elder care lawyer with Littman Krooks in New York, decided he didn't. After one year of using a cloud service to store information about all his online financial accounts, he dropped the service and came up with his own alternative. Now he keeps a Word document for each of his accounts, with the URL for the company, his username and password, the secret security question and answer. Then he stores all these documents on a password-protected section of his hard drive at the office (which his law firm backs up).

4. Back up onto a USB flash drive. You can make this thumb drive into a mini encrypted vault with a password of its own. The drawbacks: It's more cumbersome than a cloud to keep updated, and you must find someplace secure to store it.

5. Enter vital information in a looseleaf or notebook. If you don't want to go to the trouble of designing your own looseleaf system, The Beneficiary Book does it for you. It's the brainchild of Martin Kuritz, a retired financial planner, and is [available here](#) as a print edition for \$29.95 or an interactive e-book for \$19.95.

This extremely thorough book can help you create a roadmap for your agent or survivors that can be very handy when tragedy strikes. It covers not only financial records, but also things you might not have considered, like copyrights and patents that you hold, and where you keep your divorce papers and military discharge papers.

The e-book version is a downloadable PDF that users can fill in with their own information (couples can create his and hers versions). After that, they can print specific pages, then save the whole PDF to their own computer, a thumb drive or cloud storage. You also have the flexibility of printing out highly sensitive information rather than saving it electronically. (To do that, you would delete information from a specific form after you have printed it.)

6. Use an old-fashioned lock box. In combination with other methods, a fireproof safe at home or a bank safe deposit box can play an auxiliary role. Perhaps it is the ultimate depository of the paper list, flash drive or a CD with all your vital information. Or maybe this is where you put your master password, with the name of the electronic password manager that you use.

If you don't want to put all your eggs in one basket, you can mix and match these various methods--perhaps using a password manager for the pesky sign-on information you need for practically everything these days (especially if you shop online), but creating a Word file with information about your most valuable and vulnerable accounts, and storing a printout in your safe.

Whatever storage method you are considering, don't choose one that leaves you feeling technologically challenged or dependent on tools you mistrust. If you're comfortable banking online, but have not yet experienced cloud storage, for example, this might not be the occasion to start.

Once you've put everything in its place, there's one more step you need to take: let the necessary people know where to find it.

Deborah L. Jacobs, a lawyer and journalist, is the author of Estate Planning Smarts: A Practical, User-Friendly, Action-Oriented Guide (DJWorking Unlimited, 2009). An update to the book, on how the new tax law affects your estate plan, can be downloaded from the website www.estateplanningsmarts.com.