Preparing For The Ultimate Disaster

askleo.com/preparing-for-the-ultimate-disaster

March 28, 2020

Making technology convenient *and* secure is a problem we deal with daily. We make trade-offs and use techniques to hopefully strike an appropriate balance.

A more difficult dilemma that we rarely think about, however, is death or serious illness or injury. If something were to happen to you, would the people you leave behind be able to access the information they need? What happens to your encrypted data, online accounts, social media, online finances, pictures, and digital-whatever-else if you're not around to access it?

I hear regularly from people *frantically* trying to access important, sentimental, or critical data that a recently deceased or incapacitated friend or family member has locked up tightly.

It's not particularly pleasant to think about, but with all the security measures we put into place to keep bad people out, it's worth having a plan for letting good people in.

Left behind

The wife of a military member killed overseas wanted access to her husband's email account to retrieve critical information, as well as to get a glimpse into the last days of his life. The service was a free email account with no customer support. There was nothing I could do to help.

The children of an elderly gentleman needed to access his password-protected computer to retrieve the only copies of some very important family pictures. Fortunately, there are ways to break into many (though not all) Windows machines, if you have physical access.

These are just two examples of scenarios I hear regularly. Sometimes, I can help. More often, I cannot.

These are also scenarios I worry about myself. I have a large amount of encrypted data, and do many things online that require secure access. If something were to happen to me, what would my wife do?

At odds with security

This kind of disaster planning is at direct odds with the conventional wisdom that says, “Never share your password with anyone.” Yet that’s exactly what you *must* do, in case something were to happen.

It’s not an easy scenario to solve, and not all solutions work for every person…

… but solve it you must.

For those of us who would leave behind a confusing, encrypted, password-protected digital mess, it’s critical to ensure that the right people are able to access and make sense of it all.

Who do you trust?

As with so many things, it boils down to trust. Who do you trust?

And are you certain that, trusting them today, you will still trust them a year from now? Five years from now? Twenty years from now? How many friendships, relationships, and even marriages last that long?

Fortunately, you don’t have to commit to twenty years of trust. Set up properly, a timely password change or two can protect you when trust is lost. But the fact that trust *can* be lost must be built into the system.

Whenever the answer to “Do I trust them *this* much?” changes, it’s time to take action to protect yourself and find a new trustee.

It’s not always easy, but it is important.

What do you trust them with?

Once you have someone you trust, what, exactly, do you give them?

On one hand, you don’t want it to be every single password to every possible account or encrypted thing you have. That’s a maintenance nightmare, as you’d have to update your friend every time you add or change a password, without fail. Chances are you won’t, and the passwords held by your friend would quickly end up out of date.

You *definitely* don't want to use a single password everywhere. While easier to maintain with your trusted friend, it would also make it easier for a hacker to *instantly* have access to *everything* should that password ever leak out.

The ideal solution is to give them access to exactly one thing — one account or one encrypted file — in which you either automatically or periodically keep your information up-to-date.

One approach: LastPass

Using a password manager such as LastPass can help in a disaster situation.

You keep information in your LastPass vault up-to-date simply by using it. You can even add secure notes to LastPass for items that aren't covered by its online database.

LastPass has a feature called emergency access for just this scenario. You give a trusted friend the ability to *ask* for access. If you don't deny access within a certain time period — presumably because you're no longer with us — that trusted friend gets access.

That's it. When disaster strikes, your trusted contact has access to *any* of your online accounts maintained in LastPass.

Another approach: explicit encryption

I now rely on LastPass, as above, but in the past, my approach to disaster access used explicit encryption in the form of a TrueCrypt volume I used every day.

Anything important was stored inside the encrypted container. Once again, simply mounting and using it — which was a side effect of simply using the computer — naturally kept the contents up to date.

All I needed to share with my trusted friend was the location of the container and the passphrase to open it up. Once inside, everything was there, including files containing additional instructions. And once again, should trust be lost, simply change the passphrase.

There are a variety of encryption tools that work well in this scenario, including VeraCrypt, BoxCryptor, and others.

How do you trust them with it?

Simply giving someone complete access to your password manager or your entire collection of personal files can feel scary — and rightfully so. It's not something to do lightly.

To be honest, if you're not sure a specific individual can be trusted with the information, it's likely they shouldn't be. You want someone you can really trust.

One way I've found that helps just a little is to provide that critical information on paper in a sealed envelope. The implication is that you could ask for the envelope back, and, seeing it still sealed, know your trust was not misplaced.

Two-man variation

A variation of this approach is a "two-man rule". With this approach, you never give a single person your complete password, but instead select two (or more) individuals and give each of them a portion of it. Only when they agree can they assemble the pieces and gain access.

A lengthy password (or a pass*phrase)* is ideal for this, as long as the phrase is nonsensical. You should not be able to guess a missing piece of the phrase with only the portion you've been given. "Correct horse battery staple" is a good example of this, since (aside from its notoriety as an example passphrase) the words are completely unrelated to one another.

A little documentation and a lot of trust

It all boils down to a little documentation and perhaps a couple of simple additions to your existing routine. You should already be making sure that your data, passwords, and identity are secure. Building in a secure mechanism for disaster recovery isn't going to be all that difficult.

Trusting the right person requires the most thought. The rest is, essentially, just paperwork.

Responsibilities of "the keeper of technology"

My view is that as the "keeper of the technology" for your family or business, you have a *responsibility* to make sure that if something happens, they're protected.

Your needs might be different. Your solutions might be different. A CD in a safety deposit box might be enough. Perhaps keeping certain information with a family lawyer is right for you.

Or perhaps the password-sharing approach I've outlined above works for you.

But most important of all is to simply realize what *not* to do.

Don't leave your family, friends, or business without access to the information they need should you become unavailable.

That could elevate a tragedy into an even worse disaster.