

Making Sure Your Data Survives

Let's face it, we live in a digital world. Today's culture is largely defined by what happens online, whether that be social media or the workplace. Thanks to the pandemic, there's been a shift towards working remotely, so our home computers often have valuable or even sensitive information about our jobs. Even our money has turned electronic, with only 11% of the US money supply being in physical currency.

So, while we're making sure our families survive, it might be a good idea to make sure our lives survive as well, specifically our digital lives. Sometimes, we get so focused on TEOTWAWKI events, that we prep as if that's the only thing that could possibly happen to us. But I'll guarantee you, the family down the street, whose house burnt down, is as much in survival mode as you would be after an EMP. Most disasters are either regional or personal and are short-term disasters.

****PENTAGON LEAK** CHINA'S
SECRET SUPERWEAPON REVEALED**

>> CLICK TO DISCOVER MORE <<

The goal, after any of these disasters, has got to be getting our lives back to normal, or at least something that resembles the previous normal. That might mean a new normal, with significant changes from the old normal, but at least it will be a lifestyle that we can recognize, rather than living in a cave and foraging for edible plants.

In order to restore our lives to some semblance of order, we're going to need to get our digital lives back in order as well; and in order to do that, we're going to need to plan for making sure that our digital lives survive. That may not be

necessary for a TEOTWAWKI event; but it will likely be so for any other disaster.

Let me throw a hypothetical situation at you. In this scenario, you work from home, doing some highly technical and rather sensitive computer work for your employer. You're in the midst of a nasty divorce, when your house burns down in a fire. Not only do you lose everything you own, you lose records of ever owning it. On top of that, you've lost a lot of valuable work that you've done for your employer. Now what do you do?

As you can see, this hypothetical situation isn't all that far-fetched. Things like this do happen to people, causing them to lose their life's savings. In many cases, people can't even get to the assets they have left, because they've lost debit cards and can't remember their passwords. It can be a huge hassle getting banks and other financial institutions to even agree that you are you, when you need access to your own money.

Let's Start with Passwords

One chunk of electronic information that we all have to have, are our passwords. In this electronic world we live in, you can't get into anything anymore without a password. Yet keeping track of all those passwords is a challenge, in and of itself. Some people try to get by with simple passwords; but modern systems don't like those, because they are too easy for hackers to figure out. We really shouldn't use the same password over and over either, because that makes it possible for the hackers to get into everything we own, if they manage to figure it out.

The easy solution is to write our passwords down, something that many people do. But what happens if your list of passwords goes up in smoke, or is ruined in a flood, just like the rest of your house? The only way that you can prevent that

sort of catastrophe is to have a backup list of your passwords, which is somewhere other than your home; someplace you'll be able to get to, after a disaster.

A physical list is difficult to work with in this manner. It's actually much easier to use one of the online applications, which acts as a password vault for you. That will give you access to your list of passwords, no matter where you are. Just be sure to have a password for that vault, which you won't forget.

Keep in mind that banks may require more than passwords, using PIN numbers for transactions. Those are generally easier to remember, because they are short and we use them all the time. But if you're going to create a listing or database of your passwords, you might as well add those too.

Data Backups

Passwords are just the beginning of the data that we need to protect, especially if we work from home. We all have enormous quantities of data on our computers, ranging from family photos, to work that we've done for our employers. Things that used to be printed documents, which we would receive in the mail, are often nothing more than e-mail attachments, which we download to our computers, where they can easily be lost.

The old solution for this is still just as valid today, as it was 40 years ago; back up the data on your computer regularly. Fortunately, that's even easier today, with cloud computing. Several different companies offer us the means of backing up "in the cloud;" many at no additional cost to us. Apple, Google, Microsoft and Norton are some of the better-known names that offer cloud backup; but they are by no means the only companies that do.

Of course, there are those amongst us who don't like backing up on the cloud. I'm one of them. I have never liked the idea

of my data being under someone else's control, even when I worked for companies that required all our files to be on the "mainframe," before the internet became a thing.

Then again, the cloud isn't perfect. The same TEOTWAWKI events that could make it impossible for us to access our computers, could just as easily make it impossible to access the data stored on the cloud, even if we could get our personal computer working.

Going back to that old solution, the answer is to backup locally. This is also easy, with the massive external hard drives which are available. The biggest problem is remembering to do it. Then, once your backup is complete, you need to store it off-site, where it wouldn't be destroyed if your home burns down. Whether that is in a bank vault or in your garden shed, it has to be out of the house.

I keep a secondary computer in my shed, which is far enough from the house that fire won't spread easily from one to the other. That's where my own backups are stored; giving me both a convenient location and one that hopefully can't burn down with the house.

Bug Out with Your Data

The other important thing we need to be ready to do, is bug out with our most important data. Maybe it's not practical to carry a couple of external hard drives with you when you bug out, but there's nothing wrong with carrying a thumb drive, packed with your most important information. By that, I mean the things you'll need to have, in order to put your life back together. The work files and family photos come after that.

So, what sorts of information am I talking about?

- Identification documents, such as driver's licenses
- Bank account information, including online accounts

- Copies of stocks, bonds and other securities
- House and property titles
- Vehicle titles and registration
- Insurance documents
- Diplomas and degrees, as well as transcripts
- Medical records

This list is by no means complete; but it should give you a basic idea. It's amazing just how much information you can scan and fit onto one thumb drive, especially if you scan the images in black and white, rather than color. When deciding what to put on your thumb drive or drives, I'd recommend being generous in your selections. It's always better to have too much, than not enough.

If you can, back up the same information on two or three thumb drives. One should be stored in a secure area, far enough away from your home, so as to be protected by distance from any regional disaster. The others are to carry with you when you bug out. Assuming that you are married, each of you should have a copy in your bug out bag, so that if you get separated or only one of you makes it, you'll have those files.



I'd recommend storing your thumb drives in some sort of waterproof packaging or container too. While thumb drives aren't destroyed by water, nor is the data lost by them being immersed, I'd hate to take a chance on plugging one in, not realizing that it had some water inside. One good way to

waterproof them is to use an empty pill bottle. Another is to vacuum seal them, like food that is being prepared to be put in the freezer for an extended period of time. Don't use zipper storage bags though, as they aren't always waterproof.

Of course, the other problem with this, is that you'll have to find someplace with a working computer, to gain access to your data. But if we're talking about a personal or regional disaster, that really shouldn't be much of an issue. Those thumb drives might not help in the wake of a TEOTWAWKI event; but as I already said, most disasters we face are much smaller than that.