Plan for the Unthinkable

Cove Apple Club — June 23, 2021

When a loved one dies or becomes incapacitated, partners and relatives are often faced with trying to recover aspects of their digital life, including access to their priceless photos as well as their email, passwords and website logins.

If those critical details aren't properly shared, documented and stored ahead of time, it's quite often impossible to recover them. A bit of planning when times are good can help eliminate a lot of additional stress and chaos for those who need to carry on when necessary.

Here's our guide to best practices.

DEVICE CREDENTIALS

Gaining access to Apple devices **requires** that you know the **Apple ID** and **Apple ID password** for the incapacitated device owner. In addition, you also need to know the **device passcode** for each device (iPhone or iPad).

For Macs, you also need to know the **boot-up or administrative user password for the Mac**. You can find and edit this in *System Preferences* ➔ *Users & Groups* on the Mac. Click the padlock icon in the bottom-left of the Users & Groups preference pane to unlock the setting, then make any change as needed. Be sure this password is recorded somewhere safe and that you share it with your close family (see below).

If you have forgotten your Apple ID credentials, visit **iforgot.apple.com** to reset your password.

To confirm your Apple ID credentials, and set additional security and recovery options, such as a recovery email address, visit **appleid.apple.com**.

Share these details with each other, document them (explained below), and periodically refresh your memory and understanding of this critical information.

With the Apple ID credentials, you will be able to access the email, photos, Keychain, bookmarks, Notes, calendar, contacts, iCloud Drive document storage and all other data stored in Apple's ecosystem. Without them, all that data and those irreplaceable photo memories will be ***locked away forever.***

LOGINS

Whatever system your loved one uses to record website logins, you must be able to **find it** and **read it** if needed when they can't.

Ideally, that means they have ALL of their website logins and device credentials stored in a good password manager app like **1Password**, which we have recommended and used exclusively for 15 years. It's one of the best pieces of software we've ever seen in 35 years in the industry. It has never let us down, and it is only getting better. And it saves you hours of time and loads of frustration even when it's ***not*** a crisis emergency! Learn more at **1password.com**, or ask for a personalized demo!

If using a password manager app isn't possible, then make sure you all know where and how all of these important logins and other credentials are stored. Also keep a copy in a safe place, and review it at least yearly to make sure it is still legible and up-to-date.

DATA PROTECTION

Now that you both have assembled, organized, confirmed and stored all this critical data, make a plan to ***keep it safe***.

Bank safe deposit boxes are probably the ***worst*** option. They are inconvenient, costly, and in fact, they are not all that safe. In addition, updating the contents of a deposit box is not quick or easy, and then there's the matter of even remembering where the key is kept for the box!

Fireproof home document safes are relatively inexpensive, and the best models provide excellent protection against virtually every calamity that can occur to your home. Storing mission-critical documents, such as the 1Password Emergency Kit page, other credential records and instructions to relatives in case of emergency, is a good practice no matter what other measures you employ. We recommend it as a *secondary* data storage layer of protection for your most important data.

Like all aspects of these continuity plans, make sure you review what's inside the safe, where the key(s) are kept, and that the data stored in them is current.

Cloud storage options today are incredibly inexpensive, virtually unlimited in size, accessible anywhere, encrypted and secure, and designed and maintained by the most brilliant minds in the world. For Apple users, **iCloud** storage is the easiest and best choice.

For $3/month, an *entire family* can share 200Gb of iCloud storage to keep all their data, photos and important documents safe, instantly accessible, private, backed-up and encrypted.

You can also use it to keep your 1Password Emergency Kit PDF pages, wills, Durable Power of Attorney documents, medical information, and much more. **iCloud for Families** is our recommendation for storing all your mission-critical data, ***in addition*** to the 1Password app.

REVIEW REGULARLY

Whatever system you decide on, it's important to make sure that your loved ones know **what** your system is, **how** to access it, and that you **review** it with them **at least annually**.

A few minutes every few months keeping this information in mind, accessible and up-to-date will likely be a huge relief to those who will need it when the unthinkable happens.

© 2021 by Mike Sullivan | Some rights reserved