

WITH APPRECIATION TO PC MAG

<https://www.pcmag.com/feature/366465/how-to-prepare-your-digital-life-for-your-death/5>

How to Prepare Your Digital Life for Your Death

Death is inevitable. Don't make it harder on those you leave behind. Here's how to let loved ones manage passwords, sensitive data, and social media profiles after you die.

- By [Eric Ravenscraft](#)
- March 13, 2019 7:56AM EST

Our own death is as somber as it is inevitable. But as we live more of our lives online, it's more important than ever to make sure loved ones can access digital accounts when we're gone. Don't be the guy who locked cryptocurrency exchange customers out of \$250 million after his death because [only he knew the password](#).

There are a number of ways loved ones can request access to your accounts once you're gone, but they don't need that stress. Several online services allow you to designate legacy contacts or grant access after a period of inactivity. Here's how to make sure that those you leave behind are able to manage your affairs when you can't anymore.

Create a Password Manager Emergency Kit

Password managers house the keys to all your digital accounts, and you can easily pass them on to a loved one.

[1Password](#), for example, has you create [an Emergency Kit](#) when you sign up, which includes all the information someone would need to log into your account. Print it out or download a copy to a USB drive and place it somewhere safe, like a lock box, where your loved ones can access it in the event of your death.

In addition to storing passwords for your financial accounts, you can also store information like bank numbers, credit card numbers, and any other important information you might need to leave behind.

[Keeper](#) and [Dashlane](#), our Editors' Choices for [best password managers](#), have similar features. If you use Keeper, [open your vault](#) on the site, then navigate to Account > Manage Account Emergency Access. There, you can add up to five email addresses as emergency contacts. The site also allows you to set up a seven-day waiting period, so if you don't use your account in that time, your contacts are notified.

You can do the same in the Dashlane desktop app by navigating to Contacts > Emergency > Add New and entering the email address of an emergency

contact. You will then be able to set a span of time before your contacts can request access to your vault and automatically get approved.

Add a Facebook Legacy Contact

Ensuring your loved ones have access to your financial information is important, but what about social media? Preserving profiles may seem trivial, but our lives are increasingly lived online, so these accounts are the 2019 version of physical photo albums, letters, and other keepsakes.

Facebook lets you select a [legacy contact](#) who will [memorialize your account](#) and keep a pared-down version of your profile active after your death ([not before, hopefully](#)). A memorialized account will show a banner on your profile indicating that you're deceased, remove your account from public search results, and turn off birthday reminders. Friends will still be able to post messages on your timeline, if privacy settings allow it.

To set up your legacy contact, head to your [Settings page](#), and click Edit under Manage Account. In the box that appears, type the name of the person you want to be your legacy contact and click Add.

Note: This will need to be someone you're already friends with on Facebook. You can alert them that they've been selected, or not. They'll be added as a legacy contact whether you send them a message or not.

A legacy contact will be able to accept new friend requests, change your profile and cover photo, and write a pinned message once it's been memorialized. To memorialize an account, someone will need to contact Facebook directly by [heading to this page](#).

While anyone can report an account for memorialization, only the person designated as a legacy contact before the person's death will be given any access. Facebook will not appoint any legacy contacts after the fact.

You can also opt to have your account deactivated after you die; under Manage Account, scroll down to "Request account deletion."

Set Up Google's Inactive Account Manager

Google offers an Inactive Account Manager that automatically turns over control of your account to a designated person after a set period of inactivity. To set it up, [head to this page](#) and click Start. Next, decide how long you want to wait before Google declares your account inactive (by default, this is set to three months.) Below that, add or verify your own phone number and another contact or recovery email. Google will attempt to contact you multiple times via this number or email before it turns your account over to someone else. When you're done, click Next.

On the third step, click Add Person and enter the email address of the person you'd like to give control of your account to and click Next. Then, click the checkbox next to each Google service from which you want them to be able to download data. You can allow access to everything or pick and choose specific services, like YouTube. Once you're done, click Next. You'll then be able to add your contact's phone number, to help confirm their identity. Click Save.

Below this section, click Set Autoreply. This will let you set up an automatic message that will go out to anyone who emails you after your account is marked inactive. Fill out the Subject and Message field with the message you want people emailing you to receive. You can also click "Only send a response to people in my Contacts." When you're done, click Save, then click Next. The last step will let you delete your Google account three months after it's marked inactive. Enable this toggle if you want, then click Review Plan, check your choices, and click Confirm Plan.

Don't Forget About Two-Factor Authentication

If you have [two-factor authentication](#) set up on important accounts, your loved ones will need access to your phone, in addition to your username and passwords, to intercept secondary codes.

One option is to add a trusted person's fingerprint or face to your phone. Options for Android vary depending on which device you have, but a quick Google search for your specific device should put you on the right track. Apple makes things a little easier. Those who have iPhones with Touch ID can add an extra fingerprint by heading to **Settings > Touch ID & Passcode > Add a fingerprint**. If you have an iPhone X or above, add another face to Face ID; [here's how](#).

Note that even with Touch ID or Face ID set up on your iPhone, you'll need to enter the phone's passcode if the device is restarted or if it's been inactive for more than 48 hours. So it might be a good idea to also let that trusted person know your passcode, too.

Back It Up

With all these steps taken care of, a good portion of your data should be readily accessible to those you leave behind. Unfortunately, not every service offers a tidy way of granting access. That's why it's a good idea to get in the habit of saving your work to an [external hard drive](#) and [backing up your data](#). If all this is a bit overwhelming, services like [Cake](#) will handle everything for you, from end-of-life care to memorial services, and who gets all your stuff.