1Password

GUIDE

How to get started with digital estate planning

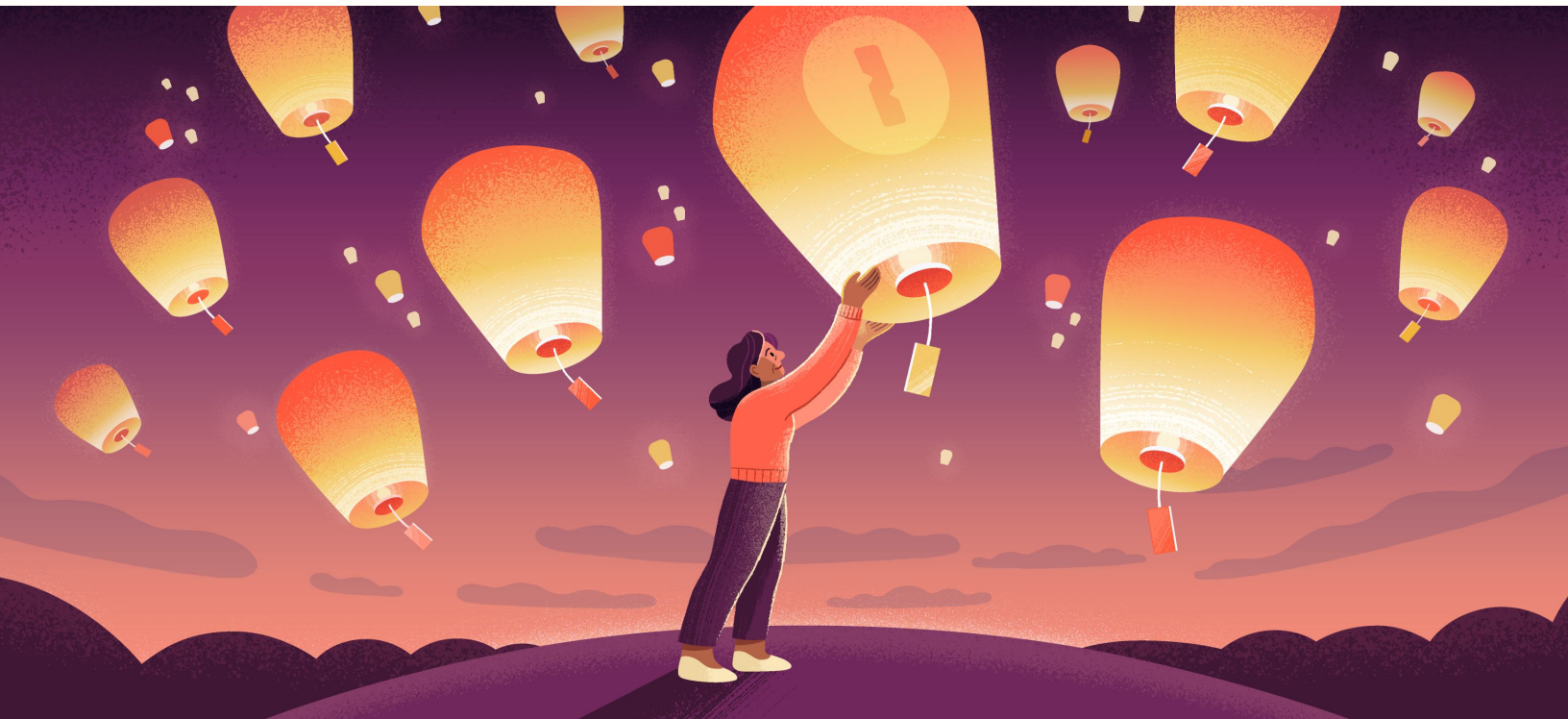

Table of contents

A message from 1Password co-founder, Sara Teare

Sara Teare
Co-founder, 1Password

Our digital life is inextricably intertwined with who we are. Embracing ways to thoughtfully pass on access to the digital resources we use every day will not only be a kindness to our loved ones, but also a core part of our legacy.

– Sara :)

1 Digital estate planning

How to share digital accounts safely

We're all familiar with wills. But have you considered your digital estate? By that, we mean all of your personal data, including any service that you log into online. Many people don't realize they need a handover plan, which can create complications for their loved ones when they pass away.

What is digital estate planning?

Digital estate planning is like traditional estate planning – but focused on everything that makes up your digital life. The process involves taking stock of your assets, including online accounts, cryptocurrencies, and data stored on personal devices, hard drives, and cloud-based services that could include personal photos, projects, and other memories . The next step is to make arrangements so that someone you trust can access your assets securely. A digital estate plan should also come with instructions that clearly explain what you would like to happen to everything you've handed over.

How to create a digital estate plan

1

Step 1: Take stock of your data

First, you need to know the breadth and depth of your data trove. Figuring this out can be tricky if your logins are scattered around on sticky notes and spreadsheets. If you use a password manager like 1Password, you can keep everything in one place and protect it all with a single password. Otherwise, you're going to have to rack your brain and pull everything together the old-fashioned way.

As you go through this process, make a note of the accounts that you consider the most important or valuable. These will probably fall into one of three buckets: money, crucial information, and ways to contact other people. You should end up with a list that covers some or all of the following:

- Banking
- Real estate accounts, inclusive of mortgage and deeds
- Government and tax-related services
- Life insurance
- Student loans
- Pension and/or retirements savings
- Cloud storage
- Email
- Social media
- Domain names and websites
- Entertainment services, like Netflix and Spotify
- Productivity apps including 1Password
- Virtual currency and investments, such as Bitcoin or stock trading accounts
- Airline accounts
- House codes (wifi, alarms, garage codes)

2

Step 2: Consider who will be inheriting your data

What makes sense to you could be confusing for someone else. A lot of people have never used a password manager, for instance. A relative might not be patient or particularly tech-savvy. Alternatively, you might have a family that is already familiar and on board with using a password manager. Regardless, you should think about the person who will be receiving your data and the type of handover they'll be able to follow.

3

Step 3: Decide how to hand over your data

There are many different ways to do this. If you use a password manager like 1Password, you could explain to your loved ones how to log into your account. The easiest way is to write some instructions and leave them in a personal safe, alongside your traditional will, or with whoever manages your will, such as an attorney or estate-planning company.

Many password managers also have built-in sharing capabilities. 1Password has vaults, for instance, that work like shareable folders. If you go down this route, you won't have to share the sensitive credentials required to log into your password manager. It will also give you more control over how much of your personal data is passed on.

1Password also has recovery codes, a unique and secure code used as a backup to help you regain access to your account in case you forget your account password or, in the case of 1Password, also lose your Emergency Kit with your Secret Key. You could opt to keep your recovery code and email account password with your will so your loved ones can use it to regain access to your 1Password account and sensitive data stored within.

Alternatively, you can export your data. Or, if you don't have a password manager, create a simple spreadsheet. A word of caution though: you'll be storing everything in a file format that anyone can read. This option might be attractive if the intended recipient doesn't have or want a password manager. The downside is that if the wrong person stumbles upon the file, they'll immediately have access to all your digital accounts. Put the file on a drive or USB stick – preferably encrypted – and keep it somewhere secure, such as a personal safe.

4

Step 4: Think about two-factor authentication

What's better than a long and random password? A long and random password backed up by two-factor authentication (2FA). The latter is a second line of digital defense. Every time you log in, the service will ask for a time-sensitive code that needs to be retrieved from a particular device or app. It's designed to ensure that you, and not a potential hacker who has somehow discovered your password, is trying to access your account. While effective, these one-time codes can be a stumbling block for friends and family trying to inherit your digital assets.

The simplest solution? Use a password manager. Some, like 1Password, can deliver time-sensitive codes whenever you need them. So if you give someone instructions to log into your account, they'll automatically inherit your 2FA codes, too. Another option is to bundle them with your passwords inside a shared vault or folder.

If you don't like these options, there are some alternatives. One-time passwords can be sent via text message, for instance. While not the most secure method – hackers have earned to intercept codes using so-called 'sim jacking' attacks – it's an easy one for relatives to understand. There are a bunch of standalone authentication apps, too, such as Authy and Google Authenticator. Some of these can be set up on multiple devices, meaning you don't have to worry about whether your loved ones can unlock your phone.

5

Step 5: Consider the information that you don't normally keep in a password manager

Password managers are a convenient place to store all kinds of sensitive information. But most people have at least one or two passwords that they prefer to keep in their brain. The password for your laptop, perhaps, or the code required to unlock your safe. Will your loved ones need this information to inherit your digital estate? If so, think about the ways you might feel comfortable handing it over. You might want to include them in your physical will, or with the instructions to log into your password manager.

6

Step 6: Look into dead man's switches

Known as a "dead man's switch," some services will automate the process of handing over data or access to your accounts. Google's Inactive Account Manager, for instance, lets you choose a custom length of time. If you don't log into your account, the timer will eventually run out and an email will be sent to a list of pre-chosen contacts. These messages can be a simple alert or contain links to data that you've stored with Google, depending on your preference. For some, this method is preferable because it doesn't require the recipient to have a password manager or understand 2FA codes.

7

Step 7: Explain your setup to the people you love and trust

Finally, you need to sit down and talk to the people who will be inheriting your accounts. If you want to use a password manager for your handover, spend a day or two walking them through the process. If you're going to leave some instructions in a safe, show them how to open it. These demonstrations will give them a chance to ask questions and raise concerns that you might not have considered.

Keep coming back to it

Our lives are always changing. You might buy a new phone, switch banks or invest in a digital currency for the first time. Technology is constantly evolving, too. More companies are thinking about security and adding two-factor authentication as an option. We're adding new features to 1Password all the time, too. It's important, therefore, to come back every so often and think about what, if anything, you need to change about your digital estate plan.

You should also keep talking to your loved ones. They might forget where you'll be leaving your handwritten instructions. Or how to access the shared vault that you've set up for them in 1Password. Others will benefit from a "trial run" every so often. These conversations can be difficult, but if you're honest and flexible with the people you care about, there's no reason why your digital handover shouldn't occur without a hitch.

Keep talking to your loved ones about where your estate planning instructions live.

Frequently asked questions (FAQs)

How do I set up a digital estate plan?

That depends on who will be inheriting your data. You could leave instructions for accessing your 1Password account in a safe, or alongside your traditional will. But if the intended recipient has never used a password manager before, you might want to consider a different form of handover.

How do you write an estate plan for digital assets?

There isn't a "correct" way to do this. Find a format that works for you and the person who will be inheriting your data. You could use a simple text file, with sections for different asset types, or a handwritten note that explains the structure of your vaults in 1Password.

What is a simple checklist to complete when using digital assets?

Create a personalized checklist by writing down all of your digital assets, including online accounts. You can do this by working through the following categories: banking, government and tax-related services, student loans, pension, mortgages and deeds, social media, email, cryptocurrencies, personal websites and domains, cloud storage, and entertainment services.

Help your loved ones by being proactive and organized with your estate plan

2 You've inherited a digital estate plan: Now what?

With each passing year, our digital lives grow in size and complexity. We open new accounts and place more value on the ones we log into and use every day. The trend has led to a rise in digital estate plans – a handover that ensures your friends and family members can take over your most precious accounts after you've gone.

Creating a plan is one challenge; figuring out what to do with someone else's is another. Maybe you've inherited one, or know a family member who plans to give you their accounts after they've passed away. Regardless, it's important to have a strategy before logging into anything that was once owned by a loved one.

1

Step 1: List the accounts in order of priority

The first step is to take stock of everything in your loved one's digital estate plan. Grab a piece of paper or create a digital document and rank the accounts in order of priority. It might seem laborious, but this exercise will help you identify which accounts require your attention first, and just as importantly, the ones that don't.

But what should be "high priority?" In general, anything money-related should go near the top of your list. That includes bank accounts, personal investments, mortgages, cryptocurrencies, and private pensions. Otherwise, the order will depend on the person who created the digital estate plan. An Instagram account will likely rank higher if your loved one was a professional influencer, for instance.

2

Step 2: Follow any written instructions

Some digital estate plans will come with instructions. If you discover any, the next step is to follow them to the best of your ability. You might find that some are impossible to carry out – for example, a company might have removed a feature that's integral to the request. In these scenarios, you'll need to pause and decide what would best honor the person and their original instruction.

3

Step 3: Consider making an announcement

Many people find community on the internet. They make friends on Twitter, join multiple subreddits on Reddit, or become an active member of various Discord servers. If your loved one had any kind of online presence, you should consider logging into their accounts and making a public announcement. That way, everyone who was close to them will be aware of what's happened.

Use your list from step one to identify and prioritize the accounts that require an announcement. Finding the words can be difficult, so take your time and ask friends and family for help. Share only what you're comfortable with and, if you've already made a decision, explain what will happen to each account moving forward. Give yourself a few hours, too, to answer questions and comments that may arise once you've made the announcement.

4

Step 4: Decide what to do with the remaining accounts

If you weren't given any instructions, or find that they only cover a subset of your loved one's accounts, you'll need to make some decisions on your own. Go through the accounts in priority order and consider the following actions:

- Do nothing (for now).
- Convert into a memorial account.
- Transfer account data.
- Transfer ownership.
- Close account.

Can't decide? Let's go through each of the options in turn.

Do nothing (for now)

There may be some accounts that you want to leave untouched – at least for now. For example, the person who passed away might have had an IFTTT account filled with "recipes" that automate complex or time-consuming tasks. You wouldn't want to edit or disable these recipes until you were absolutely sure how they worked and why they were originally created.

Whatever you do, don't rush into a decision. It's better to wait and make a good one later. If you're leaving an account up, you still have some work to do. First, you should add the account's login credentials to a password manager like 1Password. It'll make your life more convenient and serve as backup to your loved one's digital estate plan.

Secondly, you should check if the password is strong and unique. If it's not, swap it for one that is. You should then share the new password with anyone else who needs to access the account. A shared vault inside 1Password is a secure and convenient way to do this.

Finally, update any payment details associated with the account. You don't want to lose access because your loved one's bank account has been deactivated or run out of funds.

Convert into a memorial account

Some platforms, such as Facebook and Instagram, will give you the option to memorialize their account. Activating this will tweak the profile page so it's clear the original owner has passed away. On Instagram, for instance, the word "Remembering" will appear next to the person's name. It respectfully spreads the word that your loved one has passed away and ensures their posts remain accessible to the people they were originally shared with.

Transfer account data

Even with a password manager, it can be inconvenient to run someone else's account. For example, it might be tied to a specific email address or phone number that you have to monitor for important account updates. Oftentimes, it will be simpler to transfer any valuable data to another account that you control.

Let's say your loved one had a Dropbox account. You could download the files to your computer or transfer them to your own cloud storage account. Moving the files would ensure that you don't have to alternate between two accounts. It could also save you money, because it's generally cheaper to pay for a single account with a higher storage cap than two accounts with lower storage limits.

If you're going to merge accounts this way, come up with a plan for separating and filtering the data. You could make a folder for the inherited data, for instance, or use file tags to keep everything organized and searchable.

Transfer ownership to someone else

Sifting through your inherited estate plan, you might realize that some accounts would be better off in the hands of someone else. An Amazon account packed with Kindle ebooks could be perfect for a younger relative who loves reading, for instance. Similarly, you might know someone with a gaming PC who would appreciate a leveled-up Fortnite account with lots of character skins.

Use your best judgment. Before you donate an account, think about the original owner and what they would have wanted. Then, consider how other people might react to a new account owner. Few will notice or care if you hand over an account required to unlock an electric bicycle. But people might be upset if you donate a public-facing account – such as a YouTube channel or SoundCloud page – that has a large, established following.

Close the account

The fifth and final option is to close the account completely. Some will simply be redundant (if you already have a Netflix account, you likely don't need another one). But think long and hard before closing one of your loved one's accounts, because once it's gone, it will be harder if not impossible to recover. If you're not 100 percent sure, it's best to leave it alone for now.

Not sure what to do? Ask for help

If you're struggling to make a decision, reach out for advice. Friends and family members might be more familiar with a particular app or website, as well as the ramifications of closing or transferring an account. If the original owner worked with an estate planning expert, you can also reach out to them for advice.

5

Step 5: Regularly review your digital inheritance

Once you've addressed every account, set a reminder to check back in and review the ones that are still in your possession. You'll want to see if any questions or comments have been left on their public-facing pages, for instance. Similarly, it's worth looking at emails in case they've received any important messages related to their accounts.

These check-ins are a good opportunity to reassess the status of each account, too. You might have left an account untouched, but find 12 months later that you're ready to deactivate or memorialize it.

6

Step 6: Create your own digital estate plan

If you don't have one already, create your own digital estate plan. Putting one together will ensure that your loved ones don't struggle to access your accounts after you've passed away.

3

Bonus: Crypto, the latest digital asset

If you own any virtual currency, what will happen to it after you've passed away? Would your friends and family know what you owned? Or how to access the funds?

If your answer to both of these questions is "no," consider creating a handover plan. Something your loved ones can follow without being crypto-experts or diving into unfamiliar message boards for assistance.

Hot or cold?

First, understand what you're trying to hand over. Cryptocurrencies are stored in one of two ways: hot or cold wallets. Many people hear the term "wallet" and believe their funds are held inside, but that's not the case. A cryptocurrency wallet simply contains the encryption keys required to access assets on a blockchain. It's the blockchain — a digital ledger held by many people, rather than a single entity — that verifies every transaction and keeps track of who owns what.

So if you want to give someone your assets, first figure out how to give them your keys. The handover process will depend on the type of wallet or wallets you own.

Hot wallets are software-based and typically connected to the internet. Third-party exchanges such as Coinbase, Kraken, and Gemini fall into this category, as well as mainstream finance apps that support cryptocurrency like PayPal and Square's Cash App.

Cold wallets, meanwhile, have a physical component. The most popular resemble USB drives and can connect to your favorite devices directly or via Bluetooth. Most people believe they're safer than hot wallets because your private keys – the bits you're never supposed to share publicly – are always kept offline, where they're harder for cybercriminals to steal.

It might sound small, but this difference in key storage has a massive impact on how you can and should transfer ownership.

Let's start with software wallets.

Hot wallets

The first step is to check whether your preferred exchange or wallet developer has published any guidance on digital estate planning. Some companies, including Coinbase and Kraken, have support pages that address the issue. If yours doesn't, it's a good idea to reach out and ask. The company might have a formal process that isn't on their website, or they may require something you haven't considered or prepared yet.

Every exchange is different, however most have a similar stance. The ones we checked don't have a menu or settings page where you can list a preferred inheritor. Instead, they expect your loved one to contact them and supply a number of documents. Coinbase, for example, will ask for:

- A death certificate
- A last will and testament, and/or probate documents
- Government-issued photo ID of the person or people named in the above documents
- A letter signed by the person or people named in the probate documents telling Coinbase what to do with the account balance

The easiest way to prepare these documents is with an attorney or estate planning expert. Together, you can also build a digital estate plan that covers all of your most important accounts, not just the ones related to virtual currencies.

There is another way to transfer access, however: you could simply hand over the credentials required to log into your hot or cold wallet. Of course, then it's on you to protect those credentials in a robust way.

We don't recommend our users share sensitive information like their password and two-factor authentication with others as it may put their information and assets at risk," a spokesperson for KuCoin explained. "However it's worth noting that users have the final say on it, and we can hardly stop them if they insist on doing so."

The safest way to transfer access by sharing credentials is with a password manager like 1Password. Alternatively, you could write the credentials down and leave them in a personal safe alongside your traditional will, or with the person or company that manages your will.

Cold wallets

Hardware wallets require a different approach because your private keys are stored offline, rather than on a remote server. No one can access them – not even the wallet's manufacturer – unless they have physical access and know the credentials protecting both the device and your keys.

That means you're solely responsible for managing access and preparing for the handover.

You'll often be asked to create a PIN code while setting up your hardware wallet. It's similar to the code that you might set up for your phone, debit, or credit card. In addition, you'll have a recovery phrase – some companies call it a recovery code or seed – that is composed of random words. It's used to recover your private key, and therefore your digital assets, in the event that your wallet is lost.

At minimum, you'll need to hand over your recovery phrase, but we recommend adding the PIN code too, so your loved one doesn't have to buy a new physical wallet.

You should include them as part of your broader digital estate plan, if you have one. That might mean writing them into your will, which can be organized with an attorney or estate-planning expert, or sharing them via a password manager like 1Password.

There's one other way to transfer access – and it's arguably the safest of them all. Trezor, which makes the One and Model T hardware wallets, offers a recovery option called Shamir Backup. It lets you create recovery "shares" and dictate how many of them need to be combined in order to recover your private key. So if some shares are lost, your account can still be recovered with the remaining pieces. And if a hacker steals a single share, they won't have enough information to pinch your keys or, by extension, your digital assets.

If you go down this route, think long and hard about the ideal home for each share. You could give one to each of your family members, for instance. Or store one in a password manager like 1Password and another with your attorney or estate-planning expert. The choice is yours.

Hot wallets are software based; cold wallets have a physical component.

Provide context

Drafting your will or storing your credentials in 1Password isn't enough. Unless your loved one is an experienced cryptocurrency investor, they likely won't know what to do with the information you leave them. Write a brief note that explains what you're handing over and how it can be used to access your digital assets. If you're a Coinbase user, explain how the site works and where to download the mobile app. If you own a Ledger or Trezor wallet, reveal its location and how to navigate the various menus.

Then, give a brief rundown of your strategy. If you've invested in multiple cryptocoins, explain why. Do you think one has more potential than the others? And under what circumstances, if ever, were you planning to sell them? You should also explain your approach to wallets if you own more than one. Many people buy cryptocurrency through an exchange like Gemini, for example, before moving a portion to a hardware wallet for safe keeping.

You can't control what your loved ones will do with your assets. You can provide guidance, however, so they don't lose them or do something they'll later regret.

Ask the right people for help

Your cryptocurrency holdings will likely change over time. You might buy a new hardware wallet, or open another hot wallet with an exchange that's promising cheaper fees. It's important, therefore, to come back every so often and think about what you need to change or add to your handover plan.

It might also be worth having a "trial run," so your loved one can familiarize themselves with the process and ask any questions that pop up.

Finally, don't be afraid to ask about your cryptocurrency handover – but it's important to ask the right people. If you send a random tweet asking for help, you're likely to attract cybercriminals who will offer bad advice and try to steal your assets. Instead, stick to two parties: the company behind your hardware or software wallet, and an expert in drafting wills and estate planning.

4 Final Thoughts

We spend our digital lives managing dozens if not hundreds of unique passwords. The strength of our passwords protects access to our finances, online personas, and entire digital lives. Most people keep their passwords to themselves, and rightly so.

But the irony is that when we die, our passwords are the keys to granting our loved ones access to whatever we left them. And without a password-sharing plan in place, handling digital death will undoubtedly be more difficult than it needs to be.

Our digital life is inextricably intertwined with who we are. Embracing ways to thoughtfully pass on access to the digital resources we use every day will not only be a kindness to our loved ones, but also a core part of our legacy.

1Password

Trusted by over 150,000 businesses and millions of consumers, 1Password offers identity security and access management solutions built for the way people work and live today. 1Password is on a mission to eliminate the conflict between security and productivity while securing every sign-in for every app on every device. As the provider of the most-used enterprise password manager, 1Password continues to innovate on its strong foundation to offer security solutions relied upon by companies of all sizes, including Associated Press, Salesforce, GitLab, Under Armour, and Intercom.

Learn more about 1Password.