



Emergency Access — Letting a Trusted Person In

Letting a trusted person in if something happens

————— An Extended Guide · No. 1656 · PASSWORDS & SECURITY —————

Tech Made Simple. Service Made Personal.

Bill Davis — Bill's Home Tech

(330) 200-8042 · bill@billshometech.com · Atwater, Ohio

Book a visit — billshometech.com/book

What's Inside

Everything in this guide, with page numbers. Skip to whichever chapter answers your question right now.

1. A gift to the people you love	4
2. What we're really planning for	4
3. How this differs from everyday sharing	5
4. Apple's Legacy Contact	6
5. That Keychain gap, and why it matters	6
6. Google's Inactive Account Manager	7
7. Password-manager emergency access	8
8. Bitwarden's timer-based emergency access	8
9. 1Password's Emergency Kit	9
10. Other managers, same idea	10
11. The sealed-envelope approach	10
12. Choosing your trusted person	11
13. The legal picture, in plain terms	12
14. Fitting this into estate planning	12
15. A note on the password, legally	13
16. Don't forget the devices themselves	14
17. Layering for a plan that really holds	14
18. Keeping the plan current	15
19. Talking to your family about it	15
20. Avoiding scams around this planning	16
21. If you're helping a parent set this up	17

22. What your trusted person will actually do	17
23. Deciding what should happen to each account	18
24. A simple plan you can start today	18
25. Putting it all together	19
26. Frequently asked questions	20
Your Emergency-Access Cheat Sheet	20
Plain-English Word List	21
A Picture to Follow Along	23
A Second Look	24
A Note From Bill	24
Your Visit — and My Promise	25

1. A gift to the people you love

Planning emergency access is an act of kindness, not gloom.

It's a hard thing to sit with, so let's frame it the right way from the start. Setting up emergency access isn't about dwelling on the worst — it's one of the most thoughtful, loving things you can do for the people who'd have to pick up the pieces. When someone is suddenly ill, or has passed, the last thing their family needs is to be locked out of the photos, the bills, the accounts, and the records that hold a life together.

I've sat with families on both sides of this. The ones who planned ahead are spared a second ordeal on top of their grief. The ones who didn't face weeks of locked accounts, lost photos, and dead ends — at the worst possible time. The difference is a quiet afternoon of setup while things are calm. That's the whole purpose of this guide.

GOOD TO KNOW

This guide focuses on the built-in legacy and emergency features of your accounts and devices, and the planning around them. It's a companion to my family password manager guide, which goes deeper on building a shared kit.

Take it gently, a piece at a time. You don't have to do everything at once. Even setting up one of these tools puts you far ahead of most people, and each one you add is a door you've left open for someone who'll be grateful.

2. What we're really planning for

Two different situations, with different tools.

It helps to see clearly that 'something happens to you' actually covers two quite different situations, and the best tools differ for each. Sorting them out keeps your plan sensible rather than overwhelming.

- Incapacity — you're alive but temporarily or lastingly unable to manage things, through illness or injury.
- After death — you've passed, and your family needs to settle and preserve your affairs.
- The two often need different tools: some features act only after death, others while you're simply unreachable.

For incapacity, a password manager's emergency access and a sealed envelope shine, because they can let a trusted person in promptly when you need help. For after death, the

platform legacy tools from Apple and Google are built precisely for that moment. A well-rounded plan quietly covers both.

GOOD TO KNOW

A legal power of attorney covers the 'alive but unable' case, while a will and the platform legacy tools address the 'after death' case. They work together, and an attorney can make sure they fit.

3. How this differs from everyday sharing

Emergency access is a break-glass plan, not daily sharing.

If you've already set up sharing a few logins with a spouse — the subject of my sharing-passwords guide — you might wonder how this is different. Everyday sharing is for the here and now: both of you use the household bank login today. Emergency access is a sealed 'break glass in case of emergency' plan: a trusted person gets in only when a real emergency arrives, and not before.

The two complement each other. Day-to-day sharing keeps the household running while everyone's well. Emergency access is the backstop for the day someone can't manage at all. You want both, and they're set up in different places — sharing in your manager's shared vault, emergency access through special features designed to stay dormant until needed.

TIP

A good mental test: 'Who should be able to reach my things today?' is everyday sharing. 'Who should be able to reach everything if I'm suddenly gone?' is emergency access. Different questions, different answers.

This guide is about that second question — the sealed plan — and the built-in tools designed for it. Keep your everyday sharing as it is; we're adding a safety net beneath it.

4. Apple's Legacy Contact

Naming who can reach your Apple data after you're gone.

Apple offers a feature called Legacy Contact. You name one or more people you trust, and Apple gives each of them a special access key. After your death, that person can use their key, along with a copy of your death certificate, to request access to the data in your Apple account — things like your photos, documents, and messages.

- 1 On your Apple device, open Settings and tap your name.
- 2 Go to the 'Sign-In & Security' area and find 'Legacy Contact.'
- 3 Add a trusted person; Apple creates an access key for them.
- 4 Make sure they receive and safely keep that key.

It's a thoughtful, well-built feature, and setting it up takes only a few minutes. The key your contact receives is important — without it, even a named contact faces a much harder path — so make sure they store it somewhere they'll be able to find it.

WATCH OUT

Apple's Legacy Contact gives access to your account's data, but it does not hand over your saved passwords in Keychain. Your stored logins need a separate plan — a sealed envelope or your password manager's own emergency feature.

5. That Keychain gap, and why it matters

A crucial detail most people miss.

This point deserves its own moment, because it surprises people and it matters. When you use an Apple device, your saved passwords live in something called Keychain. It's wonderfully convenient — it fills in your logins automatically. But Apple's Legacy Contact, for privacy reasons, does not pass those saved passwords to your legacy contact. They can reach your photos and files, but not the list of passwords that would let them into your bank, your email, and everything else.

This isn't a flaw so much as a deliberate privacy choice — but it means that if you rely only on Legacy Contact, your family could end up with your photos yet still locked out of the accounts that matter most. That gap is exactly why this guide urges a second layer, like a dedicated password manager's emergency access or a sealed envelope.

GOOD TO KNOW

If your passwords live in Apple's Keychain, your emergency plan must include another way to pass them on. This single fact is the most important reason not to stop at Legacy Contact alone.

The simplest fixes are to keep your important passwords in a manager that has its own emergency-access feature, or to write the essentials into a sealed envelope. Either closes the Keychain gap cleanly.

6. Google's Inactive Account Manager

A plan for a Google account that goes quiet.

Google's version is called Inactive Account Manager, and it works on a clever idea: you decide how long your account can sit completely unused before Google considers it inactive. If that time passes with no sign-in, Google can notify people you've named, share chosen data with them, and even delete the account if you've asked it to.

- 1 Sign in and open your Google Account's data or security settings.
- 2 Find 'Inactive Account Manager' and choose how long of a quiet period triggers it.
- 3 Name the trusted people to notify, and pick what data they may receive.
- 4 Decide whether the account should eventually be deleted.

Because it triggers on inactivity rather than on a death certificate, it suits the reality that a Google account often simply goes silent. Google will try to reach you first — a text, an email — before acting, so an ordinary long trip won't set it off by accident.

TIP

Set the inactive period thoughtfully — long enough that a stretch away from email won't trigger it, short enough to be useful. Tell the people you name so the eventual message doesn't bewilder them.

7. Password-manager emergency access

The feature that closes the loop on your logins.

Because your passwords are the keys to everything else, a password manager's own emergency-access feature is often the heart of a good plan. The idea is that you designate a trusted person as an emergency contact, and the manager provides a controlled, safe way for them to reach your vault if you can't — without you ever simply handing over your master password.

Different managers do this in different ways, and the next chapters cover the main ones. What they share is a careful design: your person can't just stroll in, but when a genuine emergency comes, there's a built-in path that doesn't depend on you being there to let them in.

GOOD TO KNOW

This is the cleanest answer to the Keychain gap. If your important logins live in a manager with emergency access, your trusted person can reach them properly, through a feature built for exactly this.

If you don't yet use a password manager, this is one more reason to start — and my first-password-manager guide walks through choosing and setting one up gently.

8. Bitwarden's timer-based emergency access

A waiting period that keeps you in control.

Bitwarden offers an elegant emergency-access feature built around a waiting timer. You name a trusted person as an emergency contact and set a waiting period. If the day comes that they need in, they request access — and you're notified. If you don't respond to decline within the waiting period you chose, access is granted. If you're fine and simply away, you decline, and nothing happens.

- 1 In Bitwarden, open the emergency-access settings.
- 2 Invite your trusted person as an emergency contact.
- 3 Choose a waiting period — the window you'd have to decline a request.
- 4 They accept the invitation, and the plan sits dormant until needed.

The beauty of the timer is that it protects you both ways. A trusted person can always get in eventually, even if you can't respond — because you've passed, or you're in the hospital.

But if someone requested access wrongly while you're well, you'd see the alert and decline before the clock ran out.

WATCH OUT

Pick a waiting period that balances safety and usefulness: long enough that you'd notice and decline a mistaken request, short enough that a grieving family isn't left waiting far too long to reach what they need.

9. 1Password's Emergency Kit

A printed page that holds the keys.

1Password takes a different, refreshingly tangible approach with its Emergency Kit. When you set up 1Password, it offers a printable Emergency Kit — a single page holding the pieces needed to sign in, including a space for your master password. The plan is simple: you print it, write in what's needed, and store it somewhere safe that a trusted person can reach in an emergency.

- 1 In 1Password, find and print your Emergency Kit.
- 2 Write your master password in the space provided.
- 3 Store it securely — a home safe, or with your important papers.
- 4 Tell your trusted person where it is, or include it with your estate plan.

It's low-tech in the best way: no timers, no online request, just a well-kept piece of paper.

The trade-off is that it's only as safe as the place you keep it, so a locked drawer or a home safe — not a desk drawer anyone could open — is essential.

GOOD TO KNOW

1Password families can also share a vault among members, so a spouse may already have everyday access. The Emergency Kit is the backstop for the person who isn't part of that daily sharing.

10. Other managers, same idea

Whatever you use, look for the emergency feature.

Bitwarden and 1Password are two well-known examples, but the broader point is what matters: most reputable password managers offer some way to pass access to a trusted person, whether a timer-based contact, a printable kit, or a shared emergency vault. The feature names differ, but the goal is the same.

- Look in your manager's settings for words like 'emergency access,' 'trusted contact,' or 'legacy.'
- If there's a printable recovery or emergency sheet, print and store it safely.
- If there's a timer-based contact, name your person and set a sensible wait.
- If your manager has none, a sealed envelope covers the gap well.

The honest reality is that features change and vary, so the lasting advice is to check what your particular manager offers and build your plan around it. If it offers nothing suited to this, don't worry — the sealed-envelope approach in the next chapter works with any setup at all.

TIP

When you review your plan each year, re-check your manager's emergency feature too. These tools improve over time, and a feature that wasn't there before may make your plan simpler.

11. The sealed-envelope approach

The oldest method, and still a fine one.

Before any of these digital features existed, people planned for emergencies with paper, and it still works beautifully as a backstop that needs no app and no account. The idea is simple: you write down what a trusted person would need — where things are, how to get in — seal it in an envelope, and store it somewhere safe they can reach when the time comes.

- 1 Write your master password and a short map of where key things live.
- 2 Note which accounts matter most and any instructions for them.
- 3 Seal the envelope, label it clearly, and date it.
- 4 Store it in a home safe, a bank safe-deposit box, or with your attorney.

The sealed envelope's great virtue is that it covers everything, in one place, with no dependence on any company's feature. Its weakness is that it's only as safe as its hiding spot, and it can go stale — so it needs a secure home and an occasional update. Used as a backup to a digital tool, it's hard to beat.

WATCH OUT

An envelope of passwords is a real key to your life. Never leave it in an ordinary desk drawer or a labeled 'passwords' box in plain view. A locked safe or a safe-deposit box is the right home for it.

12. Choosing your trusted person

Who you name matters as much as the tool.

All of these tools come down to one decision: who do you trust with this? It's worth real thought, because you're naming someone who could, in an emergency, reach into the most private corners of your life. The right person is trustworthy without question, level-headed in a crisis, and likely to still be in your life for years to come.

- Trustworthy beyond doubt — this is the whole foundation.
- Calm and capable under stress, since they'd act at a hard time.
- Likely to outlast the plan — a spouse, an adult child, a close sibling.
- Comfortable enough with technology, or willing to call someone who is.

You can name more than one person, or different people for different tools, and sometimes that's wise — a spouse for day-to-day, an adult child as a second backstop. The key is that each person knows they've been named, and roughly what they'd need to do.

TIP

Have the conversation out loud. A trusted person who's surprised to learn their role at the worst moment is far less help than one who knew, and knew where to look, all along.

13. The legal picture, in plain terms

What the law and the fine print have to say.

Here we need to be careful and honest: whether someone may legally access your accounts can depend on the account's terms of service and on the laws of your state, and those genuinely vary. Many online services' rules technically say an account is personal and not transferable, even as the companies build legacy features to help families. The law in this area has been catching up, and it differs from place to place.

This guide can't give you legal advice, and it would be wrong to try. What it can do is point you to the right help: for anything touching your estate — who inherits what, who has authority, how your digital accounts fit your will — a licensed attorney who handles estate planning is the person to see. They can make sure your wishes are set down in a way that actually holds.

GOOD TO KNOW

Some states have adopted laws giving a named person the right to manage a deceased person's digital accounts. An estate-planning attorney will know what applies where you live and how to use it.

None of this should stop you setting up the practical tools in this guide. Think of the attorney as the person who makes your wishes legally sound, while these features make them practically workable. You want both.

14. Fitting this into estate planning

Your digital life belongs in the bigger plan.

For a long time, estate planning meant the house, the bank accounts, the will. Our lives have moved online, and now a 'digital estate' — your accounts, photos, and files — deserves a place in that planning too. The good news is that it slots in naturally alongside the traditional pieces, once you think to include it.

- Mention your digital accounts and wishes when you make or update a will.
- Tell your attorney how your passwords are stored and how access is arranged.
- Keep your sealed envelope or emergency kit with your other important papers.
- Make sure the person named in your legal documents can reach the practical tools.

The aim is that your legal plan and your practical plan point to the same person and don't contradict each other. An attorney helps you align them, so there's no painful gap between what you wished and what your family can actually do.

GOOD TO KNOW

If you're already planning a visit to an attorney for a will or power of attorney, add your digital accounts to the agenda. It's a small addition that spares your family a large headache.

15. A note on the password, legally

Why handing over a password isn't the whole answer.

A natural thought is, 'I'll just leave my passwords where my family can find them, and that's that.' Practically, that does let them in — and a sealed envelope does exactly this. But it's worth understanding that simply knowing a password isn't the same as having the legal right to use an account, especially when a company's terms say the account is personal.

In practice, families often use legacy tools and inherited passwords together, and the platform features exist precisely to give a lawful path. The takeaway isn't to worry, but to pair the practical (a password your person can reach) with the proper (legal authority through your estate plan), so your family is on solid ground, not just technically able to log in.

GOOD TO KNOW

For most families, combining a platform legacy tool, a password manager's emergency access, and a clear estate plan covers both the practical and the legal sides well. An attorney ties the legal knot.

This is one more reason to favor the built-in legacy features where they exist: they're the companies' own blessed path, designed to be lawful and respectful, not a workaround.

16. Don't forget the devices themselves

A locked phone can hide everything else.

It's easy to plan for accounts and forget the gatekeeper: the phone or computer itself. Many accounts, codes, and photos live behind a device passcode, and if that passcode is known only to you, a locked phone can quietly block your family from everything — even things you carefully planned to share.

- Make sure your trusted person can learn your device passcode when needed.
- Remember a modern phone also guards your two-factor codes and authentication apps.
- A locked, unknown passcode can undo an otherwise good plan.
- Include device passcodes in your sealed envelope or emergency notes.

This ties into my guide on a lost phone, which makes the same point from the other direction: so much hinges on the device that you must plan for someone reaching it. For emergency access, that means the passcode belongs in your sealed plan alongside your master password.

WATCH OUT

If your two-factor codes come through an app on your phone, and no one can unlock the phone, your family could be stuck even with every password. Make sure the device passcode is part of the plan.

17. Layering for a plan that really holds

No single tool covers everything — so combine a few.

By now a theme has emerged: each tool has a gap. Apple's Legacy Contact skips your passwords. Google's manager only covers Google. A manager's emergency access depends on using that manager. A sealed envelope can go stale. The answer isn't to find one perfect tool — there isn't one — but to layer two or three so that together they leave no gap.

- A password manager with emergency access, holding your important logins.
- Apple Legacy Contact and Google Inactive Account Manager, for those accounts' own data.
- A sealed envelope as a catch-all backstop, including device passcodes.
- An estate plan, through an attorney, giving it all legal footing.

You don't have to build all of this in a day. Even one layer helps. But the families who are truly covered tend to have a couple of these working together, each catching what the others miss.

GOOD TO KNOW

A good minimum for most people is a password manager with emergency access plus a sealed envelope. That pair covers your logins and your devices, and backs each other up.

18. Keeping the plan current

A plan that's gone stale can let everyone down.

An emergency-access plan is not quite set-and-forget, because the thing it points to — your accounts and passwords — keeps changing. A sealed envelope written years ago, with an old master password, could leave your family just as stuck as no plan at all. A light, regular review keeps the plan trustworthy.

- 1 Once a year, confirm your named contacts are still the right people.
- 2 Update your sealed envelope if your master password or device passcode changed.
- 3 Re-check that platform legacy settings are still in place.
- 4 Make sure your trusted person still knows their role and where to look.

Tie this to something you already do yearly — a birthday, tax season, the start of the year — so it actually happens. A few minutes keeps your plan as current as the life it's meant to protect.

TIP

If you change your master password, make updating your sealed envelope part of the same task, right then. That's the moment a plan most often quietly goes stale.

19. Talking to your family about it

The conversation that makes the plan work.

The finest plan in the world does little good if no one knows it exists. The conversation — awkward as it may feel to start — is what turns a set of settings into real protection. It needn't be heavy; frame it as practical planning, the same as telling family where the house deed or the insurance papers are kept.

- Tell your trusted person they've been named, and for what.
- Show them, in general terms, where to look and what to expect.
- Let the wider family know a plan exists, even if details stay private.
- Write down the essentials so it doesn't rest on anyone's memory.

Families often find this conversation brings relief rather than discomfort. It signals care and foresight, and it spares everyone the helpless feeling of not knowing what you would have wanted. You're handing them a map, not a burden.

GOOD TO KNOW

You control how much detail you share now versus leave sealed for later. Even just saying 'there's a plan, and here's where to find it' is a great kindness.

20. Avoiding scams around this planning

Crooks exploit worry about the future, too.

Any topic involving important accounts attracts scammers, and estate and emergency planning is no exception. Be wary of unsolicited offers to 'manage your digital legacy' or 'secure your accounts for your heirs' for a fee, especially those that arrive by email or phone out of the blue and press you to act. The legitimate tools in this guide are built into accounts you already have, and they're free.

- Set up legacy and emergency features inside your own accounts, reached by typing the address yourself.
- Be skeptical of any service cold-calling about your 'digital estate.'
- No real feature needs you to share your master password with a stranger.
- For legal help, choose an attorney you've sought out, not one who contacted you first.

WATCH OUT

A caller claiming to help 'protect your accounts for your family' who asks for your passwords or a payment is running a scam. Hang up and set these tools up yourself, or with someone you already trust.

When in doubt, slow down and check with someone you trust before acting. Genuine planning is never urgent in the way a scammer insists — it's calm, deliberate, and done on your own schedule.

21. If you're helping a parent set this up

The gentle approach when you're the family helper.

Many people come to this guide not for themselves but to help an aging parent, and that's a loving instinct. The approach is the same calm layering, with extra care for the parent's dignity and genuine wishes. This is their plan, about their life, and they should lead it for as long as they're able.

- Start from what they want — who they'd trust, what matters most to preserve.
- Set up the platform legacy tools and a manager's emergency access together.
- Create a sealed envelope and agree on a safe home for it.
- Encourage a visit to an attorney for the legal side, and offer to help arrange it.

Doing this together is also a chance to tidy up the rest — a password manager, current recovery details, a lost-phone plan. An afternoon spent this way gives a whole family peace of mind that lasts for years.

GOOD TO KNOW

If a parent has reached the point of being unable to decide or consent, that's the moment for an attorney and proper legal authority — not for quietly taking over their accounts on your own judgment.

22. What your trusted person will actually do

Walking through the moment it's needed.

It helps, when setting all this up, to picture the actual moment your plan gets used — because it reveals whether your plan is truly ready. Imagine your trusted person, at a hard time, trying to step in. What exactly do they do first? If you can answer that clearly, your plan is sound. If you're not sure, there's a gap to close.

- They need to know a plan exists and that they're the named person.
- They need to find the sealed envelope, or know how to start the emergency request.
- They need enough to unlock a device and reach your password manager.
- From there, the master password or emergency access opens the rest.

Tracing that path in your mind is the best test there is. Most plans fail not on the clever features but on a missing first step — a person who didn't know they were named, or an envelope no one could find. Walk the path, and fix whatever's unclear.

TIP

Write the first three steps your person should take, in plain words, at the top of your sealed envelope. In a stressful moment, a clear 'start here' is worth more than any feature.

23. Deciding what should happen to each account

Keep, pass on, or close — your wishes, written down.

Emergency access isn't only about getting in — it's also about what you'd want done once someone's there. Some accounts you'd want preserved, like photos a family would treasure. Others you'd want closed, like social media or subscriptions. Thinking this through, and jotting it down, spares your family from guessing at your wishes during a painful time.

- Preserve — photos, letters, documents a family would want to keep.
- Pass on — accounts or files meant for a specific person.
- Close — subscriptions and services that should simply end.
- Memorialize — some social accounts can be turned into a remembrance page.

A short written note of your wishes, kept with your sealed envelope or your estate papers, turns a mountain of uncertain decisions into a clear list your family can follow. It's a final kindness: you've made the hard choices yourself, so they don't have to.

GOOD TO KNOW

Several services let an account be 'memorialized' rather than deleted, preserving it as a place for remembrance. If that matters to you, note your preference so your family knows to ask for it.

24. A simple plan you can start today

One modest version that covers the essentials.

If the whole subject feels like a lot, here's a modest starting plan that covers the essentials and can be done in an afternoon. You can always add to it, but even this much puts you far ahead.

- 1 Put your important logins in a password manager, if they aren't already.
- 2 Turn on that manager's emergency access and name your trusted person.
- 3 Set up Apple Legacy Contact and Google Inactive Account Manager for those accounts.

4 Write a sealed envelope with your master password and device passcode, and store it safely.

5 Tell your trusted person the plan exists and where to look.

That's a genuinely strong plan, and none of its steps is hard. When you're ready, a visit to an attorney for the legal layer completes it — but the practical safety net above is yours to build today.

TIP

Do it in one sitting if you can, and finish by telling your trusted person. The 'telling someone' step is the one people skip, and it's the one that makes the whole plan real.

25. Putting it all together

The whole plan in one calm breath.

Let's bring it home. Emergency access is simply making sure that, if something happens to you, a trusted person can reach what they'll need — your accounts, your photos, your records. You do it with a few layered tools: your platform's legacy features, your password manager's emergency access, a sealed envelope, and an attorney for the legal footing. No single one is complete; together they leave no gap.

- 1 Choose a trusted person — or a few — and tell them.
- 2 Set up Apple Legacy Contact and Google Inactive Account Manager.
- 3 Turn on your password manager's emergency access for your logins.
- 4 Write a sealed envelope, including your device passcode, and store it safely.
- 5 See an attorney to give your digital estate legal footing.
- 6 Review the plan once a year and keep it current.

That's the whole of it. It's not gloomy work — it's some of the most considerate planning you can do, and finishing it brings a quiet relief. You've left the door open for the people you love, on the day they'd most need you to have thought of them.

GOOD TO KNOW

If any part of this feels like one step too many, you don't have to do it alone. Sitting down to build a calm, complete emergency-access plan is one of the most meaningful visits I do — in person or by screen-share.

26. Frequently asked questions

Quick answers to what people ask most.

Does Apple's Legacy Contact give my family my passwords? No — and this is the key catch. It shares your account data, like photos and files, but not your saved Keychain passwords. Those need a separate plan, like a manager's emergency access or a sealed envelope.

What's the difference from just sharing passwords with my spouse? Everyday sharing is for now; emergency access is a sealed backstop for when you can't manage at all. You want both, set up in different places.

Is it legal for someone to use my accounts after I'm gone? It can depend on the account's terms and your state's laws. The platform legacy tools give a lawful path, and an estate-planning attorney makes your wishes legally sound.

Do I need to pay a service for this? No. The legacy and emergency features are built into accounts you already have, and they're free. Be wary of anyone cold-calling to sell 'digital legacy' protection.

What's the simplest strong plan? A password manager with emergency access plus a sealed envelope that includes your device passcode. That pair covers your logins and devices and backs each other up.

TIP

If any of this feels like one step too many, that's exactly the kind of thing I can sit down and set up with you — in person or remotely — in about an hour.

CHEAT SHEET

Your Emergency-Access Cheat Sheet

Keep this where your plans live. It's the short list of ways to let a trusted person in if something happens to you — pick a couple that fit your life.

Platform tools (built into the account)

- Apple — Legacy Contact lets a person reach your data after you're gone (note: it can't reach your Keychain passwords).

- Google — Inactive Account Manager can share or delete your account if you stop using it.
- Set these up in each account's security settings while you're well.

Password-manager emergency access

- Bitwarden — a timer-based emergency access: your person requests, you have a set wait to decline.
- 1Password — an Emergency Kit you print and store safely for your person to find.
- Others vary — check your manager's 'emergency' or 'trusted contact' feature.

The sealed-envelope backup

- 1 Write down where things are and how to get in.
- 2 Seal it, label it, and store it somewhere safe your person can reach.
- 3 Update it when big passwords change.

The legal piece

- Accessing accounts can hinge on terms of service and state law.
- For estate planning, talk with a licensed attorney.
- Questions? Call Bill's Home Tech at (330) 200-8042.

WORDS TO KNOW

Plain-English Word List

Emergency access — An arrangement that lets a trusted person reach your accounts or data if you can't — because of illness, incapacity, or death.

Legacy Contact — An Apple feature naming a person who can request access to your account data after your death, using a key and a copy of a death certificate.

Inactive Account Manager — A Google feature that, after your account sits unused for a chosen length of time, can share chosen data with people you name or delete the account.

Emergency Kit — 1Password's printable sheet holding what's needed to sign in. You store it safely so a trusted person can find it.

Timer-based access — An emergency feature (as in Bitwarden) where a trusted person requests access and gets it after a waiting period, unless you decline in time.

Sealed envelope — A low-tech backup: written instructions and keys, sealed and stored where a trusted person can reach them when needed.

Keychain — Apple's built-in store of your saved passwords. Importantly, Apple's Legacy Contact does not give access to these passwords.

Terms of service — The rules you agreed to when you opened an account. They can affect whether someone else may legally use or access it.

Power of attorney — A legal document naming someone to act for you while you're alive but unable. Different from what takes effect after death.

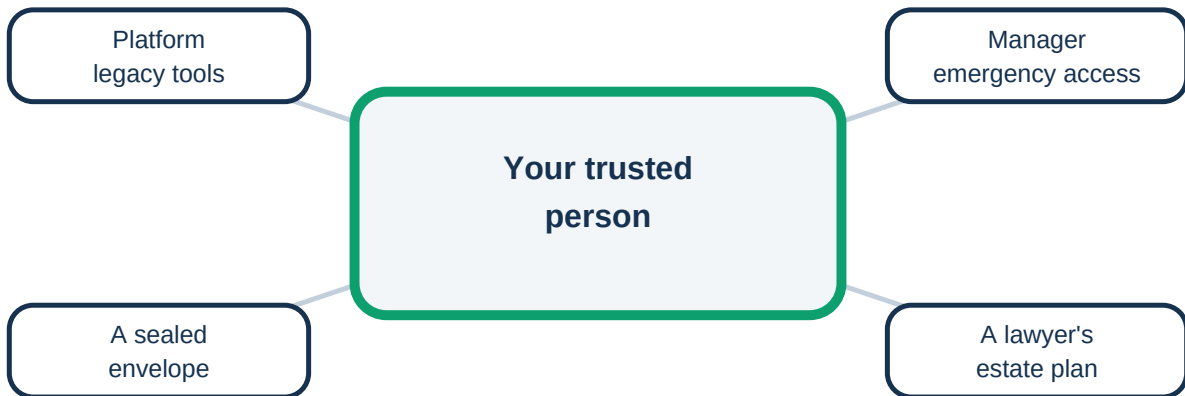
Digital estate — All your online accounts, files, and assets considered together for planning — what happens to them, and who can reach them.

AT A GLANCE

A Picture to Follow Along

Three Ways to Leave a Door Open

Pick the tools that fit your life - you can use more than one.



Layer a couple of these and the right person can always get in.

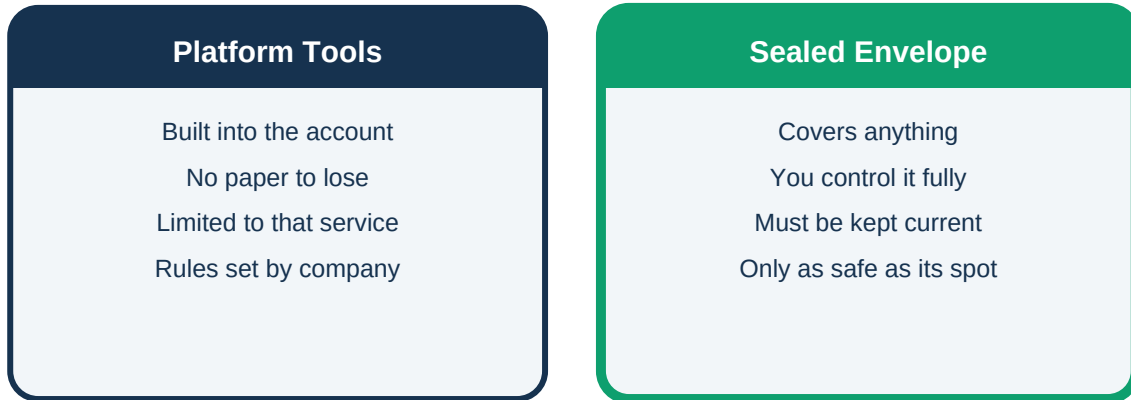
Illustration - each path leads a trusted person to what they'll need.

AT A GLANCE

A Second Look

Platform Tools vs. a Sealed Envelope

Built-in features and an old-fashioned backup each have a place.



The strongest plan usually combines a built-in tool and a paper backup.

Illustration - no single tool covers everything - layering is wise.

BEFORE YOU GO

A Note From Bill

A quick note from Bill. I write these guides to make home tech a little less frustrating, and I do my best to keep every step accurate and up to date. Still, every home, device, and setup is a bit different, so I can't promise a guide will match yours exactly or fix your particular problem. These guides are for general information only — they're not professional, legal, or financial advice, and they don't replace your device's own manual or the manufacturer's instructions. Please go slow, use your own good judgment, and use everything here at your own risk. If a step involves electrical wiring, a gas appliance, a water heater, plumbing, or climbing a ladder — or if anything just doesn't feel safe — please stop and call a licensed professional (or give me a call at 330-200-8042). Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results.



HOW I CAN HELP

Your Visit — and My Promise

In-home visit — \$99 flat for your first visit. No contracts and no surprise charges, and a 30-day follow-up is included.

Remote Support — \$49 for a screen-share session. I only connect with your permission, you watch the whole time, and you can end anytime. If I can't fix it over the screen-share, I refund the \$49 — and if it turns out you need me in person, that \$49 goes toward your visit. It's included free for Support Plan members (\$39/mo).

GOOD TO KNOW

My promise — If you're not 100% satisfied with your visit, I'll come back at no charge, or refund the full \$99. No questions, no awkwardness. That's how I'd want to be treated.

Call or text **(330) 200-8042** · Book a visit: billshometech.com/book · bill@billshometech.com

This free guide is for general information only — not professional advice, and no substitute for your device's own manual. Any prices or outside products mentioned can change; please confirm current details before you buy. Please use your own good judgment and follow it at your own risk — for anything involving electricity, gas, water, or heights, stop and call a licensed professional. Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results. © 2026 Bill's Home Tech, LLC.