



Two-Factor Codes & Locked-Out Accounts After a Death

Why a password alone no longer opens an account — and the calm, lawful ways
past the codes that lock families out

————— **An Extended Guide · No. 1811** —————

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. The Whole Plan on One Page	4
2. What Two-Factor Security Really Means	4
3. Why It Locks Out Even Rightful Family	5
4. Two Locks, and How to Open Each	5
5. When the Code Is Texted to the Phone	6
6. When the Code Comes From an App	6
7. Why the Phone and Its Passcode Matter So Much	7
8. Reading a Code Without Unlocking the Phone	8
9. What Backup and Recovery Codes Are	8
10. Where to Find the Printed Codes	9
11. When the App Is Tied to the Old Phone	9
12. Moving an Authenticator to a New Phone	10
13. The SIM Card and the Phone Number	11
14. The Phone Company's Part	11
15. What Account Recovery Is	12
16. Locked Out of an Apple Account	12
17. Apple's Recovery Key and Recovery Contact	13
18. Locked Out of a Google Account	14
19. Google Prompts, Codes, and Recovery	14
20. Locked Out of a Microsoft Account	15
21. Banks and Financial Accounts	16

22. The Order to Try	16
23. Keep the Phone Powered and Charged	17
24. The Mistakes That Make It Worse	17
25. Avoiding a Permanent Lockout	18
26. When It Is an App and There Are No Codes	19
27. The Paperwork You Will Need	19
28. Never Share a Code — the Scam Behind It	20
29. Guarding the Number Against a SIM Swap	20
30. Common Worries, Answered	21
31. Set Up Your Safety Nets Together	21
32. If You Are Settling the Estate	22
33. If You Only Do Three Things	23
34. Reaching the Data Without the Codes	23
35. A Simple Log to Keep It All Straight	24
36. Finish the Job Soon	24
Everyday Cheat Sheet	25
A Picture to Follow Along	26
A Second Look	27
A Note From Bill	27
Your Visit — and My Promise	28

THE 60-SECOND VERSION

1. The Whole Plan on One Page

If you read only one page, read this. Here is the whole idea as a short checklist.

You have the password, or even the phone, and still an account will not open. It keeps asking for a code it sent somewhere you cannot reach. This is two-factor security, and it can lock out even the rightful family after a death. Take a breath. This is a common, solvable snag, and there are calm, official ways around it.

- 1 Find the loved one's phone and keep it charged and powered on.
- 2 Watch for a texted code on the lock screen — many phones show it without unlocking.
- 3 Look for printed backup or recovery codes with their important papers.
- 4 Check whether codes come from a text message or from an app on the phone.
- 5 If you are still locked out, use the account's official recovery process.
- 6 If a step stalls, call the service's support line, or call for help rather than guessing.

GOOD TO KNOW

A locked account is rarely a lost account. Between the phone, a printed backup code, and the official recovery process, there is almost always a door. It just takes patience to find the right one.

The rest of this guide explains what two-factor is, where the codes go, and exactly what to do for the major services. Take it one page at a time. There is no silly question here.

WHAT THIS IS

2. What Two-Factor Security Really Means

Two-factor security, sometimes written as two-step or 2FA, is simply a second lock on an account. The first lock is the password, something the person knew. The second is something the person had — usually their phone. After you type the password, the account asks for a short code that proves you are holding the right phone.

It was built to stop thieves. Even someone who steals a password cannot get in without that second step. For the living, it is a wonderful protection. The trouble comes after a death, when the second step is tied to a phone or a number the family may not be able to reach. The lock meant to stop strangers now stands in front of the people who loved the owner.

- The first step is the password — something your loved one knew.

- The second step is a code — proof of something they had, usually the phone.
- You often need both to get in, which is why a password alone is not enough.

GOOD TO KNOW

If an account asks for a code after you enter a correct password, that account has two-factor turned on. Recognizing it is the first step to getting past it.

WHY LOCKED OUT

3. Why It Locks Out Even Rightful Family

It can feel almost unkind that a security feature keeps out a grieving spouse. But two-factor cannot tell the difference between a thief and a widow. It only knows whether the person signing in can produce the second step. If the code goes to a phone you cannot unlock, the account treats you exactly as it would treat a stranger.

This is not a flaw you did anything to cause, and it is not personal. The companies built these walls high on purpose, because accounts hold money, memories, and private lives. The same height that protected your loved one is now the height you must find a way around — through the proper doors, not over the wall.

GOOD TO KNOW

The companies are not trying to keep families out. The official recovery paths exist precisely so the rightful person can get in when the second step is out of reach.

So the goal is never to defeat the second step by force. It is to reach the code another way, or to prove through the official process that you are the rightful person. Both are patient paths, and both work more often than families expect.

THE BIG IDEA

4. Two Locks, and How to Open Each

The whole subject becomes simpler once you picture two separate locks. To get into most accounts you need to open both. If you can open both, you are in. If you can open only one, you are stuck at the second — and the rest of this guide is about opening that second lock, in each of the ways it can appear.

- Lock one: the password. You may already have it, or reset it through the email.
- Lock two: the second step. A texted code, an app code, or a printed backup code.

- If the password is reset but the second step still blocks you, that is the knot to untie. Knowing which lock is stopping you tells you exactly where to aim. If you have no password, the email guide and the password guide help there. If you have the password but cannot produce the code, you are in the right place, on the right page.

TIP

When an account rejects you, notice carefully what it is asking for. 'Wrong password' and 'enter the code we sent' are two different problems with two different answers.

TEXTED CODES

5. When the Code Is Texted to the Phone

The most common second step is a code sent by text message to the phone number on the account. You sign in, and a six-digit code arrives as a text. This is the easiest kind to get past after a death, because the text lands on the phone, and many phones show it without even unlocking.

That is why the single most useful thing you can do is keep your loved one's phone charged and powered on. As long as the phone has signal and the number is still active with the carrier, the codes keep arriving. If you can see the text, you can read the code and finish signing in, even from another device.

- A texted code goes to the phone number on the account.
- The phone must have power and signal to receive it.
- Many phones show the code on the lock screen without unlocking.
- Keeping the phone line active for a while keeps this door open.

GOOD TO KNOW

A texted code is usually the gentlest kind to reach. If the phone is on and the line is live, you may never need the harder recovery paths at all.

APP CODES

6. When the Code Comes From an App

The other common second step is an authenticator app — a small app on the phone that generates a fresh code every short while, with no text message involved. Common ones are named Google Authenticator, Microsoft Authenticator, Authy, and Duo. If your loved one used one, the codes live inside that app, on that phone.

This kind is harder, because the codes are not texted anywhere — they are made on the device itself. To read them, you generally need to get into the phone, which means knowing the passcode. If the phone is locked and you do not have the passcode, the app codes may be out of reach, and you will lean on backup codes or the official recovery process instead.

WATCH OUT

Do not factory-reset a phone that holds an authenticator app. A reset erases the app and the codes inside it, which can lock you out of every account that relied on it.

- An authenticator app makes codes on the phone, with no text message.
- Reading the codes usually means unlocking the phone with the passcode.
- If the phone is locked, backup codes or official recovery become the route.

THE PHONE

7. Why the Phone and Its Passcode Matter So Much

By now a pattern is clear: the phone sits at the center of almost every second step. It receives the texts. It holds the authenticator app. It is often the trusted device an account recognizes. If you can get into the phone, most two-factor walls fall away. If you cannot, you work around them with backup codes and recovery.

This is why the phone's passcode — the four or six digits that unlock it — is so precious. A known passcode is close to a master key for two-factor. If your loved one ever shared it, or wrote it down, that small number may save you hours. A companion guide covers getting into a late spouse's phone in full.

GOOD TO KNOW

The phone passcode and the account passwords are different things. The passcode opens the handset; the passwords open the accounts. For two-factor, the passcode is often the one that matters most.

If you do have the passcode, use it gently and soon, before the phone restarts. A phone that powers off and back on will often demand the account password again before it fully opens, which can close this easy door.

THE LOCK SCREEN

8. Reading a Code Without Unlocking the Phone

Here is a small detail that rescues many families. Most phones, by default, show the beginning of a new text message right on the lock screen — the screen you see before you unlock. A texted code often appears there in full, or at least enough of it to read, without you ever needing the passcode.

- 1 Keep the phone charged and powered on, with the lock screen showing.
- 2 On another device, begin signing in to the account you need.
- 3 When it says it has sent a code, watch the loved one's phone.
- 4 Read the code as it appears on the lock screen as a new message.
- 5 Type that code into the sign-in to finish.

TIP

If the code does not appear on the lock screen, the phone may be set to hide message previews. That does not mean it is lost — it only means you will need the passcode or a backup code instead.

This trick works only for texted codes, not for an authenticator app, whose codes live inside the locked app. But for the most common kind of two-factor, it is often all that stands between you and the account.

BACKUP CODES

9. What Backup and Recovery Codes Are

When someone turns on two-factor, most services offer a set of backup codes, sometimes called recovery codes. These are a short list of one-time codes, each usable once in place of a texted or app code. They exist for exactly this situation: the day the phone is lost, broken, or locked. If your loved one saved theirs, they are a quiet gift to you.

Each code works a single time and then is spent. A typical list holds eight or ten of them. People are told to print the list or write it down and keep it somewhere safe — with a will, in a home safe, or in a binder of important papers. So the first thing to do is simply look for that list.

- Backup codes stand in for the second step when the phone is out of reach.
- Each code works once, then is used up.
- They are usually printed or written and stored with important papers.
- A single unused code may be all you need to get into an account.

GOOD TO KNOW

Finding a printed sheet of backup codes can turn a locked account into an open one in seconds. It is always worth searching the papers before starting a long recovery request.

BACKUP CODES

10. Where to Find the Printed Codes

Backup codes are only useful if you can find them, so it helps to know where people tend to keep them. They may be on a printed sheet, handwritten in a notebook, or saved as a file or a photo on the computer. A patient search often turns one up where you least expect it.

- 1 Look through the binder or folder of important papers and the home safe.
- 2 Check a notebook or an address book near the computer or the desk.
- 3 On the computer, look for a saved file or printout named for the service.
- 4 If you can reach the email, search it for the words 'backup codes' or 'recovery codes.'
- 5 Ask other family members whether a list was ever shared with them.

TIP

If you find codes, use them one at a time and cross each off as you go, since each works only once. Save the unused ones carefully until the account is fully settled.

If no codes turn up, do not lose heart. Many people never saved them, and that is normal. You still have the phone, the lock-screen trick, and the official recovery process ahead, and one of those will usually open the door.

AUTH APPS

11. When the App Is Tied to the Old Phone

Authenticator apps are the trickiest kind of two-factor after a death, because older ones kept their codes only on the single phone where they were set up. If that phone is locked or lost, the codes inside can be out of reach, and the accounts that relied on them become hard to open. It is worth understanding this clearly so you aim your effort well.

The newer versions of several authenticator apps now offer a cloud backup, meaning the codes can be restored to a new phone if you have the account they are linked to. Whether that helps depends on which app your loved one used and whether they turned backup on. When it is not available, backup codes and official recovery become your route.

- Older authenticator apps stored codes only on the one phone.
- Some newer versions can restore codes from a cloud backup to a new phone.
- Whether backup was on depends on the app and your loved one's settings.
- If the codes cannot be restored, use backup codes or the account's recovery process.

GOOD TO KNOW

Even if an authenticator app's codes are truly lost, each account behind it almost always has its own separate recovery process. The app being gone is a setback, not the end of the road.

AUTH APPS

12. Moving an Authenticator to a New Phone

If you can get into the loved one's phone and want to keep their accounts reachable, you may be able to move the authenticator app's codes to a phone of your own. This is delicate work, and it is only worth attempting if you have the passcode and some patience. If it feels beyond you, a helper can do it in a short visit.

- 1 Unlock the old phone and open its authenticator app.
- 2 Look in the app's menu for an export, transfer, or move option.
- 3 Follow its steps to move the codes to the new phone, often by scanning a code on screen.
- 4 Confirm the codes now appear on the new phone before you set the old one aside.
- 5 Keep the old phone untouched until you are sure the move worked.

WATCH OUT

Do not reset, wipe, or trade in the old phone until every account is confirmed working on the new one. The old phone is the only copy of those codes until the move is finished.

Not every app supports a simple move, and not every account survives it cleanly. If some accounts resist, fall back to their own recovery processes. The goal is reaching the accounts, however you get there, not perfecting the transfer.

THE SIM

13. The SIM Card and the Phone Number

The phone number itself deserves special attention, because for texted codes, the number is the second step. That number lives on a small chip inside the phone called the SIM card, tied to the carrier — the phone company that provides the service. Keep the number alive, and texted codes keep arriving. Cancel it, and that door closes.

This is why rushing to cancel the phone line can backfire. Many accounts send their codes to that number, and once it is gone, you can no longer receive them. A little patience with the line can make resetting a dozen other accounts far smoother. The companion phone guide covers the carrier's role in more depth.

- The phone number is the second step for any texted code.
- The number lives on the SIM card and belongs to the carrier.
- Cancelling the line stops the codes from arriving.
- Keeping it active for a while eases resetting other accounts.

TIP

Before you cancel a phone line, make a list of every account that still texts a code to that number. Close those loose ends first, while the codes can still reach you.

THE CARRIER

14. The Phone Company's Part

The carrier cannot open your loved one's accounts, but it controls the number those accounts text, so it matters here. If the SIM is damaged or the phone is broken, the carrier can sometimes move the number to a new SIM or a new line, which can bring the codes back to a working phone. They have their own process for a deceased customer.

Moving a number is done carefully, because criminals abuse it — the so-called SIM swap. So the carrier will ask for a death certificate and proof that you are authorized, often an executor or next of kin. Be ready for that, and know the caution is there to protect your loved one's number from a thief, not to obstruct you.

WATCH OUT

A SIM swap is also a scammer's trick to steal codes. Never approve a number transfer you did not request, and be patient when the carrier asks for proof before moving the number for you.

If keeping the number matters for reaching accounts, speak with the carrier before cancelling anything. Explain plainly that you need the number live for a time to settle the estate. They handle such requests often, and will tell you the steps.

RECOVERY FLOWS

15. What Account Recovery Is

When neither the phone nor a backup code works, nearly every major service offers one more path: account recovery. This is the official 'I have lost my second step' process, where the service helps the rightful person back in after extra checks. It is slower than the other paths, because the service is being careful, but it is a real and reliable door.

Recovery usually means answering questions about the account, confirming a backup email, or waiting out a set period while the service makes sure no thief is at work. Each company runs it a little differently, and the next few pages walk through the big ones. The common thread is patience: recovery rewards the steady, not the hurried.

GOOD TO KNOW

Account recovery is designed for exactly your situation — a rightful person locked out of the second step. It is not a loophole or a trick; it is the front door the company built for this.

- Recovery is the official path when the phone and backup codes fail.
- It may ask account questions, a backup email, or a waiting period.
- It is slower by design, to keep thieves from abusing it.
- Every major service has one, though each works a little differently.

APPLE

16. Locked Out of an Apple Account

An Apple Account, once called an Apple ID, guards a person's iCloud photos, backups, and more, and Apple protects it firmly with two-factor. If you are locked out, the gentlest path is the one set up in advance: an Apple Legacy Contact, who uses an access key and a death certificate to reach the account data. The companion phone guide covers that in full.

If there is no Legacy Contact, Apple has an account recovery process for a living person who is locked out, and Apple Support can sometimes help a family member with a death certificate and proof of relationship. Apple reviews these carefully, so expect a wait

measured in days, not minutes, and keep notes of every call.

GOOD TO KNOW

Apple's Legacy Contact path reaches the account data even when the phone and its codes are out of reach. If your loved one set one up, start there before anything else.

- Best path: an Apple Legacy Contact named in advance, with the access key.
- No Legacy Contact: Apple account recovery, or Apple Support with a death certificate.
- Apple reviews requests by hand, so patience is part of the process.

APPLE

17. Apple's Recovery Key and Recovery Contact

Apple offers two advance safety nets that sometimes help a family, if your loved one set them up. One is a Recovery Key, a long code that can restore access to the account. The other is a Recovery Contact, a trusted person who can help the owner back in. These are separate from the Legacy Contact, and worth knowing about.

If your loved one wrote down a Recovery Key, or named you as a Recovery Contact, that may open a door. If they did not, these cannot be set up after the fact, and you fall back to account recovery or Apple Support. As ever, the paths set up in advance are the smooth ones; the rest take more patience.

TIP

Search the important papers for a long printed code labeled as a recovery key. If you find one, keep it safe and mention it when you contact Apple — it can shorten the road considerably.

- A Recovery Key is a long code that can restore account access.
- A Recovery Contact is a trusted person who can help with recovery.
- Both must have been set up in advance; neither can be added afterward.
- Without them, account recovery or Apple Support is the route.

GOOGLE

18. Locked Out of a Google Account

A Google account holds Gmail, Google Photos, and on an Android phone, much of the person's digital life. Google protects it with two-factor that may use a texted code, a prompt on the phone, or an authenticator app. If your loved one set up Google's Inactive Account Manager in advance, naming you, you simply receive a download of the data they chose — the smoothest path by far.

If not, Google has a formal request process for a deceased person's account, covered in the email and phone guides. Google will never hand over the password or the account itself. What it may do, after careful review, is provide a download of the data or help close the account. For two-factor specifically, that download sidesteps the codes entirely.

GOOD TO KNOW

Because Google's deceased-user request gives you a data download rather than a login, it skips the two-factor wall altogether. You never have to produce a code to receive the download.

- Smoothest: a prearranged Inactive Account Manager plan naming you.
- Otherwise: Google's deceased-user request for a data download.
- Google never gives the password, so you work with the download.
- The download route avoids the two-factor codes entirely.

GOOGLE

19. Google Prompts, Codes, and Recovery

If you happen to know the Google password and want to sign in directly, you may still hit the second step. Google may send a code by text, show a 'yes, it's me' prompt on the phone, or ask for an authenticator code. Knowing the phone passcode, and keeping the phone on, lets you answer most of these the same way a lock-screen code works.

If you are stuck, Google's own account recovery can help a rightful person back in by asking questions about the account and confirming a recovery email or phone. It may ask you to wait a period while it checks. Answer from a device and place the account has been used before, if you can, as that helps Google trust the request.

TIP

If your loved one listed a recovery email or phone you can reach, Google's recovery can send the code there instead of to the locked phone. Check what the recovery options offer before giving up.

As always, do not guess the password many times over. Repeated wrong tries make Google more suspicious, not less, and can slow the very recovery you are trying to complete.

MICROSOFT

20. Locked Out of a Microsoft Account

A Microsoft account covers Outlook.com mail, OneDrive files, and more, and it too uses two-factor. The hard truth, covered in the email guide, is that Microsoft generally will not give account information to anyone but the account holder, and it has no next-of-kin form or legacy contact. There is no special bereavement team to hand over the second step.

If you know the password, you may be able to sign in and, if the account still asks for a code, use Microsoft's own recovery, which can rely on a recovery code or a backup email the owner set. If you do not know the password, reaching the contents generally requires a court order, and even that is not guaranteed.

GOOD TO KNOW

A Microsoft account closes on its own after about two years of no sign-in. If you cannot get in and the contents are not essential, letting it lapse is a valid, restful choice.

- Microsoft has no next-of-kin form or legacy contact for two-factor.
- With the password, its recovery may use a recovery code or backup email.
- Without the password, contents generally need a court order.
- An untouched account closes by itself after about two years.

BANKS

21. Banks and Financial Accounts

Banks and investment accounts guard their sign-ins tightly, and most text a code before letting anyone in. Here, though, the two-factor wall matters less than you might fear, because you should not be signing into a deceased person's bank account to act on it anyway. The bank wants to hear from you through its own estate process, not through a login.

So rather than wrestling with a bank's texted code, call the bank, tell them of the death, and ask for their estate or bereavement department. With a death certificate and proof you are the executor or next of kin, they will open the account to you properly, through the right channel, which protects the estate far better than logging in ever could.

WATCH OUT

Do not log in and move money from a deceased person's bank account, even if you can. It can look as though the person acted after death and can seriously complicate the estate. Use the bank's estate process instead.

For banks, then, a locked login is almost a blessing in disguise: it nudges you toward the proper path. Let the two-factor wall stand, and go in through the front door the bank built for exactly this.

A CALM ORDER

22. The Order to Try

With the pieces laid out, here is a calm order to work through, so you are never wondering what comes next. You do not have to finish it in a day. Just take the next open step, and leave the rest for another sitting.

- 1 Keep the phone charged and powered on; do not reset or wipe it.
- 2 Try the lock-screen trick for any texted code.
- 3 Search for printed backup or recovery codes among the papers.
- 4 Check whether codes come from a text or an authenticator app, and plan accordingly.
- 5 If still locked out, start the account's official recovery or bereavement process.
- 6 If any step stalls, call the service's support line, or call for local help.

GOOD TO KNOW

Most families find that the phone plus a backup code opens the accounts that matter most, and the official recovery is only needed for the stubborn few.

Keep a simple written log as you go: which account, what you tried, and the date. It keeps a tangled task from blurring together and helps anyone who assists you pick up where you left off.

KEEP IT ON

23. Keep the Phone Powered and Charged

If there is one habit that helps more than any other, it is simply keeping your loved one's phone alive. So much of two-factor runs through that device that a dead or powered-off phone can turn an easy task hard. Treat the phone as a working tool you need, not just a keepsake to set aside.

- Keep the phone plugged in or topped up so it never dies while you work.
- Do not power it off, and avoid letting it restart, which can demand the account password.
- Leave it where it keeps a signal, so texted codes keep arriving.
- Set it aside only once you have what you need from the accounts.

WATCH OUT

A phone that restarts — from a dead battery or an automatic update — often asks for the account password again, not just the passcode. Keep it charged so that door stays open.

This one small discipline, keeping the phone on and charged, quietly preserves every texted-code path at once. It costs nothing and spares you a great deal of harder work later.

WHAT NOT TO DO

24. The Mistakes That Make It Worse

Two-factor is forgiving if you are patient and unforgiving if you rush. A few common mistakes can turn a reachable account into a locked one, so they are worth naming plainly. None of these are things anyone would do knowing better; they happen in the fog of grief and hurry.

- Do not factory-reset the phone — it erases authenticator codes and texted-code access.
- Do not guess a password many times — it can lock the account and slow recovery.
- Do not cancel the phone line before you have reset the accounts that text it.

- Do not approve any sign-in or number transfer you did not start — that is a scammer's move.

WATCH OUT

The single most damaging mistake is wiping the phone to 'start clean.' On an authenticator-based account, that can lock you out permanently, with no way back. When unsure, leave the phone exactly as it is.

When in doubt, stop and set the phone down. Almost nothing about this is so urgent that it cannot wait a day while you get the right help. Slowing down is itself a form of protection.

AVOID LOCKOUT

25. Avoiding a Permanent Lockout

The fear that haunts this whole subject is a permanent lockout — an account that can never be opened. It is rare, and it almost always comes from a preventable mistake rather than bad luck. Understanding how it happens is the surest way to avoid it. In nearly every case, a door remains if you simply do not slam the others shut.

Permanent lockout usually follows one of a few events: the phone with the only authenticator codes is wiped or discarded, the phone number is cancelled before accounts are reset, and no backup codes were ever saved. Any one of these alone rarely ends things. It is doing several in a hurry that closes the last door.

GOOD TO KNOW

As long as the phone exists and has not been wiped, the number is still live, or a backup code survives somewhere, the account is almost certainly still reachable. Protect those three things and you protect your options.

- Keep the phone intact and unwiped.
- Keep the number active until accounts are reset.
- Hold on to any backup codes you find.
- Start official recovery before closing any of these doors.

NO BACKUP

26. When It Is an App and There Are No Codes

The hardest single case is this: the second step is an authenticator app, the phone is locked with no passcode, and no backup codes were ever saved. It feels like a dead end, and it is the tightest knot in this whole guide. But even here, there is usually a thread to pull, because each account behind the app has its own separate recovery.

The move is to leave the app aside and go to each account directly, using its 'lost my authenticator' or account-recovery option. Many offer an alternative: a code to a backup email, a set of questions, or a waiting period. It is slower, one account at a time, but it routes around the missing app rather than fighting it.

TIP

Start with the email account, because once you control the email, many other accounts can send their recovery codes there instead of to the lost app. The email is the thread that unravels the rest.

If even that stalls, the official bereavement processes — Apple's, Google's, and the rest — can reach the data without the app at all. The missing authenticator is a hard obstacle, not a final wall. Take the accounts one at a time, and lean on help.

DOCUMENTS

27. The Paperwork You Will Need

Every official recovery and bereavement path asks for the same small stack of documents. Gathering these once, early, means you are ready for each service instead of scrambling at every step. A funeral home can usually help you order the certified copies you will need.

- A certified death certificate — the official state copy, not a home printout.
- Proof you are the surviving spouse, such as a marriage certificate.
- Court papers naming you as executor, or the will if it names you.
- Your own photo identification.

Order several certified death certificates at once, because each company may want its own copy, and the same stack serves the bank, the carrier, and the pension too. For online forms, a clear scan or photo of each document is usually enough; keep the paper originals for offices that insist on seeing them.

TIP

If you were named executor, say so plainly in every request. It is the word that most often moves a cautious company from a polite refusal to a path forward.

STAY SAFE

28. Never Share a Code — the Scam Behind It

There is a cruel scam built around the very codes you are working with, and the newly bereaved are a favorite target. A stranger calls or messages, claims to be from a bank, a company, or even a government office, and asks you to read back a code that just arrived. The moment you do, they are into the account. No honest company ever asks for a code this way.

- A caller claims to be from a service and asks you to read back a code you received.
- A message says you must 'verify' by sharing a code to keep an account open.
- A stranger asks for a code to 'confirm your identity' before helping with the estate.
- A pop-up or link urges you to enter a code on a page you did not go to yourself.

WATCH OUT

A two-factor code is a key. Reading it aloud to a caller is like handing a stranger your house key. No real company will ever ask you to share one. If someone does, hang up.

If a message or call tries to rush or frighten you into sharing a code, that urgency is itself the warning. Slow down, hang up, and if you are unsure, call the company back on a number you look up yourself. Taking your time is a form of protection.

STAY SAFE

29. Guarding the Number Against a SIM Swap

Because so many codes travel by text, criminals try to steal the phone number itself, a trick called a SIM swap. They convince the carrier to move the number to a phone they control, and suddenly all the texted codes go to them. A death, sadly, can create an opening for this if the estate is slow to act.

- 1 Tell the carrier of the death and ask what protections they can place on the number.
- 2 Ask whether a PIN or passcode can be required before any changes to the line.
- 3 Watch for a sudden loss of signal on the phone, which can signal a swap in progress.
- 4 Never approve a number transfer or new SIM you did not request.

GOOD TO KNOW

If the phone abruptly loses all service for no clear reason, call the carrier at once from another phone. A sudden dead line can be the first sign someone is trying to steal the number.

Protecting the number protects every account that texts a code to it. A short call to the carrier to lock the line down is time very well spent while the estate is being settled.

COMMON WORRIES

30. Common Worries, Answered

The same few questions come up for almost everyone facing a two-factor wall. Here are plain answers to the ones asked most.

- Is a locked account gone for good? Almost never. Between the phone, backup codes, and recovery, there is usually a door.
- Can the company just turn off two-factor for me? No. They route you through recovery or bereavement instead, which is safer for everyone.
- Do I need the phone to be unlocked? For texted codes, often not — the lock screen may show them. For app codes, usually yes.
- Is it too late if I already cancelled the phone line? Often not. Many accounts have another recovery path. Ask before giving up.

GOOD TO KNOW

The most common regret is acting in a hurry — wiping a phone or cancelling a line too soon. Patience almost always leaves more doors open than haste does.

If your worry is not here, it is almost certainly one a helper has met before. You are not the first to face a locked account, and you will not be the last.

FOR COUPLES

31. Set Up Your Safety Nets Together

If both partners are still here, the kindest thing you can do is make sure two-factor would never lock the survivor out. It takes one quiet afternoon, and it removes the single most frustrating obstacle a grieving spouse usually meets. You are each promising to make the hardest day a little easier for the other.

- On each account, print the backup codes and store them together with your papers.

- Set each other as the recovery email and recovery phone where the account allows.
- On Apple, name each other as a Recovery Contact and a Legacy Contact.
- Write down both phone passcodes and seal them with the important papers.

GOOD TO KNOW

Doing this together often surfaces small surprises — an account with no backup codes, a recovery phone that is out of date. An afternoon of it quietly strengthens your shared security too.

Planning for a day you hope is far off can feel tender. But couples who do it almost always feel relief rather than sadness — the quiet comfort of knowing the other will not be left locked out at the worst possible time.

FOR THE EXECUTOR

32. If You Are Settling the Estate

If you are the executor rather than the spouse, the paths are the same, but your authority rests on the court papers naming you. Lead with those in every request. The services and the carrier all respond far better to a clearly named executor than to a well-meaning relative without legal standing.

- 1 Keep the letters of administration or the will naming you close at hand for every request.
- 2 Secure the phone first — charged, on, and unwiped — since so many codes run through it.
- 3 Reach the email account early, because it unlocks recovery for many others.
- 4 Keep a written log of every account, code, request, and conversation, with dates.

WATCH OUT

Work in order of urgency: accounts that hold money or keep charging a card first, memories next, the rest after. You do not have to open everything at once.

Be gentle with yourself. This is heavy work at a hard time, often for a grieving family counting on you. You do not have to be an expert — only patient, and willing to take it one careful step at a time.

A SIMPLE START

33. If You Only Do Three Things

Perhaps this all feels like a great deal. That is understandable, and you do not have to do it all at once. If you do only three things, do these, and you will have protected the most important ground.

- 1 Keep the phone charged, powered on, and unwiped.
- 2 Search for any printed backup or recovery codes among the important papers.
- 3 Keep the phone line active until you have reset the accounts that text it.

Those three steps preserve nearly every door two-factor might ask you to open. Everything else in this guide — the recovery flows, the carrier, the authenticator transfer — becomes far easier once these are in hand.

TIP

Done is better than perfect. Simply keeping the phone on and the line live today puts you ahead of most families, and it buys you time to tackle the rest at your own pace.

ANOTHER WAY IN

34. Reaching the Data Without the Codes

It is worth remembering that getting past two-factor is not always necessary. For the things families most want — the photos, the mail, the memories — the official bereavement processes often hand over the data directly, with no code required. That can be simpler than fighting the second step at all.

- Apple's Legacy Contact path reaches iCloud data with an access key and a death certificate.
- Google's deceased-user request provides a data download, skipping the codes entirely.
- A bank's estate process opens the account to you properly, without any login.
- These routes aim at the data, not the device, so a locked second step does not block them.

GOOD TO KNOW

When the goal is the photos and the records rather than the live account, the bereavement download routes often beat wrestling with two-factor. Ask what the data request offers before you spend days on codes.

So if a second step has you truly stuck, step back and ask what you actually need. Often it is the contents, and there is a calmer door to those that leaves the codes behind entirely. The companion email and phone guides walk those routes in full.

KEEP A LOG

35. A Simple Log to Keep It All Straight

Two-factor turns settling accounts into many small steps across many weeks — a code tried here, a recovery request filed there, a carrier call somewhere else. It is easy to lose track. A plain written log keeps the whole effort from blurring together and is a real gift to anyone who helps you.

- 1 Start a page with the date, the account, and what you tried.
- 2 Note how each account's second step works — text, app, or backup code.
- 3 Write down any recovery request you filed and its reference number.
- 4 Mark what you are still waiting on, so nothing slips away unfinished.
- 5 Keep the log with the death certificates and estate papers.

TIP

One line per account — the service, how its second step works, and where it stands — becomes the backbone of settling everything. The log you keep here serves the whole estate.

This small habit pays off most on the day you must explain where things stand, to an attorney, a family member, or a helper. A clear log turns a swirl of codes and calls into an orderly record anyone can follow.

FINISH THE JOB

36. Finish the Job Soon

You now know the shape of the whole task. Two-factor is a second lock. The codes come by text, by an app, or on a printed backup list. The phone and its passcode sit at the center, the phone number matters, and the official recovery paths catch what the rest cannot. It is a lot to hold at a hard time, and you do not have to hold it alone.

If any step gives you pause — a code you cannot reach, an authenticator you cannot move, a recovery that will not budge, or simply the weight of facing it by yourself — that is exactly the kind of thing I help neighbors with. There is no question too small, and no grief I

have not sat beside before.

GOOD TO KNOW

You do not have to remember all of it. You just have to remember you can call. Friendly, in-home help, and I come to you — (330) 200-8042.

A locked-out account feels like a closed door, but it is almost always one you can open with patience and the right key. Keep the phone alive, find the backup codes, use the proper recovery, and lean on help where you need it. Take the time. Finish the job.

CHEAT SHEET

Everyday Cheat Sheet

Keep this page handy. It points you straight to what to do for each task. I want to... Do this
Keep the phone alive Charged, powered on, and unwiped — most codes run through it
Read a texted code Many phones show it on the lock screen without unlocking Find
backup codes A printed or written list of one-time codes with the papers Handle an app's
codes Authenticator codes live on the phone; some can move to a new one Mind the
phone number Keep the line active until accounts that text a code are reset Use account
recovery Apple, Google, and Microsoft each have an official locked-out path Leave banks
to the estate Do not log in and move money; use the bank's estate process Never share a
code No real company asks you to read back a code — hang up Get help Call Bill: (330)
200-8042

AT A GLANCE

A Picture to Follow Along

Where the Second Step Lives

A password alone no longer opens an account — a second step guards the door.

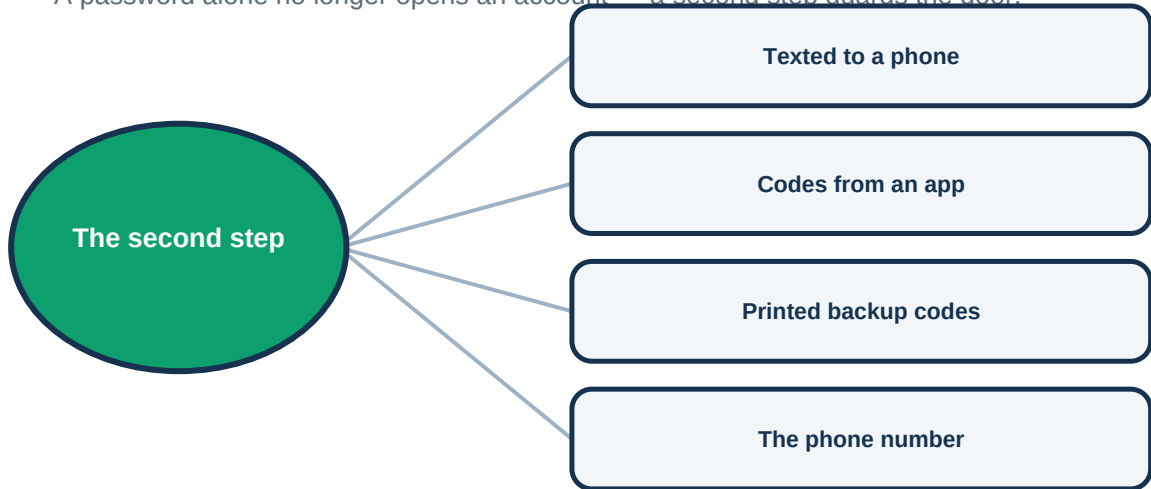


Illustration — a schematic. Set-up screens differ; each takes only a few minutes.

AT A GLANCE

A Second Look

The Calm Order to Try

Do one box at a time — there is no rush, and no wrong pace.

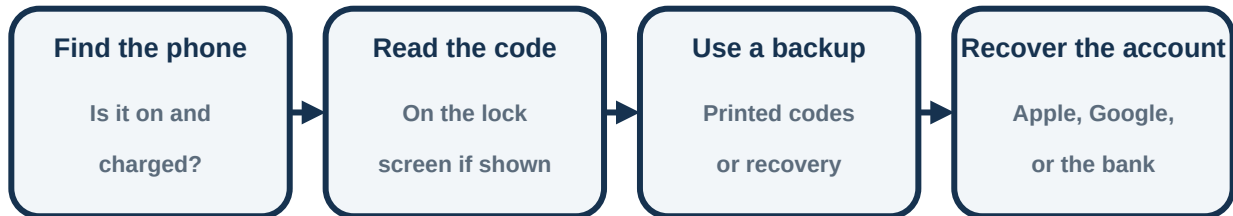


Illustration — a schematic. The order is a suggestion; do one box at a time.

A schematic of the plan — company steps vary; the order does not have to.

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.