



Recovery Codes — The Backup Keys You Must Not Lose

The backup keys you must not lose

————— An Extended Guide · No. 1651 · 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. What recovery codes actually are	4
2. Why losing them can lock you out for good	4
3. When and where the codes appear	5
4. The two-copy rule	6
5. A password manager is the easiest copy	6
6. Printing a copy, done safely	7
7. Places that seem handy but aren't	7
8. Finding your codes at Google	8
9. Recovery options at Apple	9
10. Recovery options at Microsoft	9
11. Codes on your other accounts	10
12. Setting a backup phone or second method	10
13. Test it before you need it	11
14. Using a code when you're truly locked out	12
15. When someone might have seen your codes	12
16. How codes fit with passkeys	13
17. Account recovery when the codes are gone too	13
18. Helping a spouse or parent set theirs up	14
19. A safe yearly check	14
20. Scams that target your codes	15
21. Common worries, answered plainly	16

22. Why the codes look so strange	16
23. Keeping a simple index of what's protected	17
24. What to do the day you get a new phone	17
25. Why email codes come first	18
26. A gentle version for the computer-shy	19
27. The quiet confidence this buys	19
28. Putting it all together	20
Your Recovery-Codes 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. What recovery codes actually are

A spare key for the day your usual sign-in isn't available.

When you turn on two-factor sign-in or set up a passkey, the service usually hands you a small list of backup codes. Think of them as spare keys to your own front door. Most days you walk in with your main key — your phone, your fingerprint, a tapped code. But if that main key is lost, broken, or left behind, the spare is what gets you back inside.

Each code is a short string of numbers or letters. You're given several at once — often eight or ten — because each one works only a single time. You use one, cross it off, and the rest wait for next time. They are deliberately plain so you can read one over the phone or type it from a printed page.

GOOD TO KNOW

Recovery codes and backup codes are two names for the same thing. Apple also offers a stronger version it calls a Recovery Key. We'll cover each of the big services by name later in this guide.

You may never need them. But the one time you do — a dead phone on vacation, a stolen handset, a new device that won't receive your text — a recovery code is the difference between a two-minute fix and being locked out of your own email, photos, and banking.

2. Why losing them can lock you out for good

The protection that keeps thieves out can keep you out too.

Two-factor sign-in works because nobody can get into your account with your password alone — they'd also need the second step. That's wonderful protection against a thief. But it cuts both ways. If you lose your phone and you also never saved your backup codes, you can be in exactly the thief's position: you have the password, but not the second key.

Some services offer a slow, careful recovery process to get you back in. Others, when the protection is turned up high, offer very little. Apple is blunt about this: if you set a Recovery Key and then lose both your trusted devices and that key, Apple itself cannot let you back in. The account, and everything in it, is gone.

WATCH OUT

This is not a scare tactic. People do permanently lose access to a lifetime of email and photos this way. The good news is that saving your codes once, properly, removes the risk almost entirely.

So the stakes are simple. Recovery codes are low effort to save and enormously costly to be without. Ten minutes of care now buys you a safety net that lasts for years.

3. When and where the codes appear

They flash by during setup — catch them while you can.

The codes show up at one specific moment: when you first turn on two-factor sign-in, or when you set up a passkey or a recovery key. The screen typically says something like 'Save your backup codes' and lists them. There's usually a button to download, print, or copy them.

The catch is that this screen often appears only once. Many services will not show you the same codes again for safety reasons. If you breeze past it — tapping 'Done' to get on with your day — the codes vanish, and getting a fresh set means going back into your settings on purpose.

- 1 Watch for a screen titled 'Backup codes,' 'Recovery codes,' or 'Save these.'
- 2 Don't tap 'Done' or 'Continue' until the codes are saved somewhere safe.
- 3 Use the 'Download' or 'Print' button if one is offered.
- 4 Then, and only then, finish the setup.

WATCH OUT

If you've already turned on two-factor in the past and didn't save your codes, don't worry. You can go back into each account's security settings and generate a fresh set anytime. We'll walk through where to find that.

4. The two-copy rule

One safe copy is good; two is how you sleep at night.

Here's the single habit that makes all of this reliable: keep two copies of your codes, in two different kinds of places. If one copy is ever lost — a drowned phone, a misplaced folder — the other is still standing. One copy is a big step up from none. Two copies is where real peace of mind begins.

- Copy one: inside your password manager, in the same entry as that account's login.
- Copy two: printed on paper, kept where you store important documents.
- Optional third: told to, or left with, a trusted family member.

The two copies should fail in different ways. A password manager protects you if the house floods; a printed page protects you if you're ever locked out of the very password manager that holds everything. Spreading your eggs across two baskets is the whole point.

GOOD TO KNOW

This is the same logic as keeping a spare house key with a neighbor instead of only under the mat. If the mat washes away, you still have a way in.

5. A password manager is the easiest copy

It keeps your codes and your login together, locked behind one key.

If you already use a password manager — or you've been meaning to — it's the most convenient place to keep recovery codes. You store them right alongside the username and password for that account, so everything about getting in lives in one entry. When you're locked out, you open the manager, find the account, and the codes are waiting.

- 1 Open the saved entry for the account, or create one.
- 2 Find the 'Notes' field, or a 'one-time passwords' section.
- 3 Paste or type the codes in, clearly labeled 'Backup codes.'
- 4 Save. The manager encrypts it behind your master password.

The codes are then protected by the same strong lock as the rest of your manager. Just remember the one catch: if you lose access to the password manager itself, this copy goes with it. That's exactly why you also keep a printed copy, which doesn't depend on any app.

TIP

Store the codes for your email account in your password manager AND on paper. Email is the master key to most of your other accounts, so its backup codes are the ones you least want to be without.

6. Printing a copy, done safely

Paper has no battery and never needs a password.

A printed page is the sturdiest backup there is. It can't run out of charge, it won't be locked behind a forgotten password, and it survives a dead phone or a crashed computer. The trade is that paper can be read by anyone who finds it, so where you keep it matters as much as printing it.

- Print the codes, then write on the page which account they belong to and the date.
- Keep the page where you store other important documents, not loose on a desk.
- A small home safe or a lockbox is ideal; a locked drawer is good.
- If you shred old versions, make sure you've generated and saved new codes first.

WATCH OUT

Never tape your codes to the monitor, leave them under the keyboard, or tuck them in your wallet. A sticky note by the screen defeats the entire purpose — it's like leaving the spare key in the lock.

If you keep a binder or folder of important papers — insurance, the will, account numbers — that's a natural home for a printed codes page. Anyone you'd trust with those papers is someone you'd trust with these.

7. Places that seem handy but aren't

The convenient spots are usually the unsafe ones.

It's worth naming the tempting-but-risky places, because they feel natural in the moment and quietly undo your protection. The rule of thumb: if a code is somewhere a stranger could stumble on it, or somewhere that disappears when your phone does, it's the wrong place.

- A sticky note on or near the screen — anyone in your home or a visitor can see it.
- A plain file on your desktop named 'passwords' or 'codes' — the first place a thief looks.

- Only in your memory — these codes are long and random on purpose; you won't recall them.
- Only a photo on the same phone you're protecting — lose the phone and you lose both.
- An email to yourself with the codes in the body — your email is the account most worth breaking into.

None of these is foolish; they're just the easy path. The small extra effort of a password manager and a printed page is what turns a backup from theater into something that actually works when the day comes.

GOOD TO KNOW

Emailing codes to yourself is an especially common one. The trouble is that if someone ever gets into your email, they'd find the keys to everything else sitting right there.

8. Finding your codes at Google

Backup codes live under your 2-Step Verification settings.

Google keeps backup codes with its two-step settings. You can get there on a computer or phone by typing myaccount.google.com into your browser yourself and signing in. Look for 'Security' and then '2-Step Verification.' You may be asked to confirm your password again, which is normal.

- 1 Go to myaccount.google.com and open 'Security.'
- 2 Choose '2-Step Verification' and confirm your password if asked.
- 3 Scroll to 'Backup codes' and open it.
- 4 Choose to view, download, or print your set of codes.
- 5 Save them to your password manager and print a copy.

If you've used some codes before, Google lets you generate a fresh set, which cancels the old ones. That's the right move if you ever think an old printed page went missing — new codes make the lost ones worthless.

TIP

Exact wording and menu names shift over time, so look for the ideas — 'Security,' 'Two-step,' 'Backup codes' — rather than an exact label. If you can't find it, Google's own help pages, reached by typing the address yourself, walk through it.

9. Recovery options at Apple

Apple leans on trusted devices, with a Recovery Key as the strong backup.

Apple does things a little differently. Instead of a list of backup codes, it mostly relies on your trusted devices — your iPhone, iPad, or Mac — to confirm it's you. As long as you have one of those and can unlock it, you can usually get back in. For most people, that plus a trusted phone number is enough.

For extra protection, Apple offers a Recovery Key: a single long code you turn on in your settings. It's powerful, and it's meant for people who want the tightest control. The serious catch is that once a Recovery Key is on, you are responsible for it — lose it and your trusted devices, and Apple cannot recover the account for you.

- 1 On your iPhone or iPad, open Settings and tap your name at the top.
- 2 Tap 'Sign-In & Security.'
- 3 Look for 'Recovery Key' or 'Account Recovery.'
- 4 If you turn on a Recovery Key, write it down in two safe places immediately.

WATCH OUT

Only turn on a Recovery Key if you're confident you'll keep it safe forever. For many folks, a trusted device plus a recovery contact is plenty, without the risk of a key that locks even Apple out.

10. Recovery options at Microsoft

Microsoft gives a single recovery code to store away.

Microsoft accounts — the ones you use for Outlook, Office, Xbox, or signing into Windows — offer a recovery code as well. You'll find it in your account's security settings on the web. Type account.microsoft.com into your browser yourself and sign in, then look under 'Security' for the advanced options.

- 1 Go to account.microsoft.com and open 'Security.'
- 2 Open 'Advanced security options' or similar.
- 3 Find the recovery code section and generate or view your code.
- 4 Save it to your password manager and print a copy.

Microsoft also leans heavily on a backup email address and phone number, so make sure those are set and current. If your main way in fails, Microsoft can send a code to that backup contact to verify it's really you.

GOOD TO KNOW

Because this account can be what signs you into your Windows computer itself, being locked out of it can mean being locked out of your PC. That makes its recovery code one of the important ones to keep.

11. Codes on your other accounts

Banks, social media, and shopping sites offer them too.

Google, Apple, and Microsoft are the big three, but the same idea shows up across the accounts you use every day. Many banks, your social media, your shopping accounts, and your password manager all offer backup or recovery codes once you turn on two-factor sign-in. The menus differ, but the location is predictable.

- Look under 'Security,' 'Sign-in,' or 'Two-factor authentication.'
- Find a link labeled 'Backup codes,' 'Recovery codes,' or 'Recovery options.'
- Generate the set, then save and print it like the others.
- Give special care to your email and anything financial.

You don't have to do every account in one afternoon. Start with the ones that would hurt most to lose — email first, then banking, then anything holding years of photos or messages. Work down from there as you have time.

TIP

Your password manager itself has recovery options worth saving, because it holds everything else. Treat its backup code or recovery kit as the most precious one of all.

12. Setting a backup phone or second method

A second way in means one failure doesn't strand you.

Recovery codes are your paper safety net, but most services also let you add a second live method — a backup phone number, a second email, or a trusted device. These work hand in hand with your codes. The principle is the same as the two-copy rule: more than one way in means a single problem can't lock you out.

- Add a backup phone number, such as a spouse's or a landline that can take a call.
- Add a second email address you can actually get into.
- Keep a second trusted device signed in, like an iPad as well as an iPhone.

- On some services, name a recovery contact — a person who can help verify you. Pick backups you'll still have access to a year from now. A backup phone number for a line you cancel, or a second email you forget the password to, is no help at all. Steady, lasting options are the ones worth adding.

GOOD TO KNOW

A backup method and a stack of codes aren't either-or. Set both. The codes cover you when no phone is reachable; the backup method covers you when you simply left your main phone at home.

13. Test it before you need it

A two-minute dry run turns worry into confidence.

The best time to learn how a recovery code works is a calm afternoon, not a panicked moment in an airport. So once you've saved your codes, do a short dry run. The goal is simply to see the screens and prove to yourself that the spare key really does open the door.

- 1 Sign out of one account on a spare device, or use a private browser window.
- 2 Sign back in with your password.
- 3 At the second-step screen, choose 'Try another way' or 'Can't use your phone?'
- 4 Pick 'Enter a backup code' and type one of yours in.
- 5 Confirm you're back in, then cross that used code off your list.

Once you've done it once, the process stops being mysterious. You'll know exactly which buttons to look for and that your saved codes are the right ones — which is the whole point of testing.

TIP

Remember each code is single-use. The one you test is now spent, so note it as used. If you're running low on unused codes, generate a fresh set and save those.

14. Using a code when you're truly locked out

The calm steps for the moment it actually counts.

Say the day comes: your phone is gone, and you need into your email from a borrowed computer. This is exactly what the codes are for, and the path is short. Take a breath — you prepared for this.

- 1 Go to the service by typing its address yourself and sign in with your password.
- 2 When it asks for the second step, look for 'Try another way,' 'More options,' or 'Can't use your phone?'
- 3 Choose 'Enter a backup code.'
- 4 Open your saved codes and type in one you haven't used.
- 5 Once in, consider generating fresh codes and updating your backup phone.

If you're on someone else's computer, sign out fully when you're done and don't let the browser save your password. Borrowed devices are fine in a pinch, as long as you leave nothing behind.

WATCH OUT

Never read your backup codes aloud to someone who called you claiming to be 'support.' Real services don't phone you asking for a code. A caller who wants your code is a thief, every time.

15. When someone might have seen your codes

Generating a fresh set makes the old ones worthless.

Codes aren't forever-fixed. If you ever worry an old printed page went astray, that a repair shop had your phone, or that you typed codes into a page you're no longer sure was genuine, you can wipe the slate clean. Generating a new set instantly cancels every old code, so even if someone has the old list, it opens nothing.

- 1 Sign into the account's security settings.
- 2 Find the backup or recovery codes section.
- 3 Choose 'Generate new codes' or 'Get new codes.'
- 4 Save and print the new set, and safely discard the old page.

This is a reassuring thing to know. You're never stuck with a compromised list — a few taps replaces it entirely. Make it a habit to regenerate after any time your codes might have been exposed.

GOOD TO KNOW

Generating new codes does not change your password or your phone's role. It only swaps out the backup list, so your day-to-day sign-in is unaffected.

16. How codes fit with passkeys

The newer sign-in still wants a backup behind it.

Passkeys are the newer way to sign in, replacing the password with your phone or computer's own unlock — a face, a fingerprint, a PIN. They're genuinely easier and safer day to day. But they raise the same question as two-factor: what happens if the device holding your passkey is lost or broken?

That's why, even with passkeys, services still want you to have a backup — recovery codes, a second passkey on another device, or a trusted phone number. A passkey is a lovely front door, but you still want a spare key in case you can't reach that door.

- Many passkeys sync across your devices, so a second device can be your backup.
- Keep recovery codes anyway, for the case where no device is reachable.
- Setting a passkey on both a phone and a tablet is a simple, strong safety net.

TIP

My guide on setting up passkeys walks through turning them on across Google, Apple, Microsoft, and Amazon — and where each one tucks away its backup options.

17. Account recovery when the codes are gone too

There's often still a path back, if you've laid the groundwork.

Suppose the worst mix: no phone, no saved codes. Is it hopeless? Often not — but how well it goes depends almost entirely on what you set up beforehand. Services offer an account recovery process, where they try hard to confirm you really are the owner before letting you back in.

That process leans on the backups you put in place: a recovery email, a trusted phone number, a recovery contact, or a device you're still signed into somewhere. The more of those that are current, the faster and friendlier recovery is. With none of them, recovery can be slow, frustrating, or — in the strictest setups — impossible.

- Keep a recovery email and phone number set and current on every important account.
- Stay signed in on at least one spare device when you can.
- On Apple and some others, add a recovery contact — a trusted person who can help.
- Never assume recovery will be easy; it rewards preparation, not hope.

GOOD TO KNOW

My guide on getting back into a locked Apple or Google account walks through each service's recovery path in detail, for the day you need it.

18. Helping a spouse or parent set theirs up

Backups that outlast any one person's memory.

If you manage accounts for a spouse or an aging parent, recovery codes deserve a spot in your family's important papers. The aim is that getting back into a loved one's email or bank doesn't depend on one person remembering where a single phone's codes were hidden.

- Keep each person's codes in a shared, trusted place like a family password manager.
- Print a copy for the household document binder, labeled by account.
- Write down which backup phone and email each account uses.
- Make sure at least two people know where all of this lives.

For someone with memory trouble, this is especially kind. They don't have to remember anything — the codes and the plan are written down where a trusted helper can follow them. It turns a possible crisis into a simple lookup.

TIP

My guides on the family password manager and on emergency access pair naturally with this — they cover exactly how to share these codes with the right people and no one else.

19. A safe yearly check

Five minutes to be sure your net still holds.

Recovery codes don't expire, but the world around them changes — you get a new phone, cancel an old number, switch email providers. A quick yearly look keeps your safety net in good repair. Tie it to something you already do each year so it's easy to remember.

- 1 Confirm your backup phone number and recovery email are still ones you can reach.

- 2 Check that your printed codes page is where it should be and still readable.
- 3 Make sure your password manager still holds the codes for your key accounts.
- 4 If you've used several codes, generate a fresh set and save it.

That's the whole routine. In five minutes you've confirmed that the spare keys to your digital life are still cut, still fit, and still where you'll find them.

GOOD TO KNOW

A birthday or tax season makes a fine annual reminder. The exact date doesn't matter; doing it once a year does.

20. Scams that target your codes

Crooks know the codes are the keys, so they ask for them.

Because a recovery code is a working key to your account, scammers would love to trick you into handing one over. The play is almost always the same: someone contacts you pretending to be support, creates a sense of urgency, and asks you to read them 'a code to verify your account.' The moment you do, they're in.

- No real company will ever call, text, or email you asking for a backup or recovery code.
- A code is for YOU to type into the official site, never to read aloud to a caller.
- Urgency — 'your account will be deleted, act now' — is the scammer's main tool.
- If a message pushes you to a link, don't use it; type the address yourself.

WATCH OUT

If anyone asks you for a verification or recovery code — by phone, text, or email — stop. That request alone tells you it's a scam. Hang up, and if you're unsure, call the company using a number from its official site.

When something feels off, you can always slow down and ask someone you trust, or give me a call. Checking first is free, and it's never the wrong move.

21. Common worries, answered plainly

The questions folks ask most about backup codes.

What if I run out of codes? You generate a fresh set anytime from the account's security settings. The new set replaces the old one.

Do codes expire on their own? Generally no. They stay valid until you use them or until you generate a new set that cancels them.

Is it safe to keep them in a password manager? Yes — that's one of the best places, because they're locked behind your master password. Just keep a printed copy too, in case you're ever locked out of the manager itself.

Can I reuse a code? No. Each one works a single time, which is exactly why you're given several.

TIP

If any of this feels like one step too many, that's the kind of thing I sit down and do with folks all the time — in person or over a screen-share, usually in under an hour.

22. Why the codes look so strange

The randomness is a feature, not a quirk.

People sometimes squint at a backup code — a jumble like '4k9t-2m7q' — and wonder why it can't be something friendlier. The answer is that the strangeness is exactly the protection. A code made of random letters and numbers can't be guessed, worked out from your birthday, or stumbled onto. Its whole job is to be unguessable.

That same randomness is why you can't rely on memory and must write the codes down. No one is meant to memorize them. They're designed to be read off a page or copied from your password manager, used once, and crossed off. Trying to recall them is like trying to recite a phone book — not the point.

- The dashes and spacing are just there to make the code easier to read and type.
- Upper- and lower-case usually don't matter, but type them as shown to be safe.
- A zero and the letter O can look alike — if a code is rejected, try the other.

GOOD TO KNOW

If you're ever unsure whether a character is a one or a lowercase L, a zero or an O, type carefully and try the alternative if the first attempt fails. The code is either accepted or not — there's no penalty for a careful second try.

23. Keeping a simple index of what's protected

A one-page map so nothing falls through the cracks.

As you turn on two-factor sign-in across your accounts, it helps to keep a simple list of which accounts are protected and where their codes live. Not the codes themselves on this list — just a map. It answers the question 'did I ever set that up?' without you having to hunt.

- List each important account: email, bank, password manager, shopping.
- Note whether two-factor is on and where the backup codes are kept.
- Note the backup phone number and recovery email for each.
- Keep this map with your important papers, next to the codes page.

This small sheet turns a vague sense of 'I think most of my accounts are covered' into a clear picture. It also makes the yearly check quick, because you're working from a list instead of trying to remember every account you own.

TIP

Start the list with your email and your password manager. Those two are the master keys — if they're protected and backed up, you've covered the accounts that matter most.

24. What to do the day you get a new phone

A smooth handoff so your second step moves with you.

A new phone is the moment recovery codes earn their keep, because your authenticator app and your passkeys may live on the old one. A little planning makes the switch painless. The order matters: set up the new phone before you wipe or give away the old one, while you still have both in hand.

- 1 Keep the old phone working until the new one is fully set up.
- 2 Move or re-add your authenticator app and passkeys to the new phone.
- 3 Sign into your key accounts on the new phone to confirm the second step works.

4 Only then wipe the old phone and pass it on.

If the old phone is already gone — lost, broken, or traded in before you thought of this — that's precisely when your saved backup codes rescue you. You sign in on the new phone with your password and a backup code, then set the second step up fresh.

WATCH OUT

Don't factory-reset or hand over an old phone until you've confirmed your accounts work on the new one. Many a lockout starts with wiping the only device that held the second step.

25. Why email codes come first

Your inbox is the key that opens all the others.

If you do nothing else from this guide, secure and back up your email account first. The reason is simple: almost every other account lets you reset your password by sending a link to your email. Whoever controls your inbox can walk into your other accounts one by one. It is the master key.

So your email's backup codes are the single most important set to save in two places. If you were ever locked out of email with no way back in, it wouldn't just be lost messages — it could cascade into your banking, your shopping, and everything else that resets through that inbox.

- Turn on two-factor sign-in for your email if it isn't already.
- Save its backup codes in your password manager AND on paper.
- Set a recovery phone and a second email for the account.
- Treat these as the crown jewels of your backups.

TIP

My guide on locking down your email as the master key goes deeper on this one account. It's the highest-value hour you can spend on your digital safety.

26. A gentle version for the computer-shy

This is still for you — here's the unhurried path.

If you don't spend much time on a computer, the idea of hunting through security menus can feel like a wall. It's more approachable than it sounds, and you don't have to become an expert to be protected. The safety a backup code gives you is just as real however you get there.

You can take it one account at a time, starting with email, with no rush to finish in a day. You can write your codes by hand on paper if typing them into an app feels like too much at first. And you can ask a trusted family member, or me, to sit with you and do it together the first time, so you see how it works.

- One account per sitting is perfectly fine — email first.
- Hand-writing codes on labeled paper is a valid, sturdy backup.
- A trusted helper or a short visit can get you started with confidence.

TIP

This is one of the most satisfying things to knock out together. If you'd like company for it — in person or by screen-share — that's exactly the kind of visit I do all the time.

27. The quiet confidence this buys

What it feels like to have a net under you.

There's a particular calm that comes from knowing you're covered. Once your codes are saved and your backups are set, a lost or broken phone stops being a source of dread. It becomes a minor errand — annoying, maybe, but not frightening, because you know the spare key is in the drawer.

That calm is really what all of this is for. Two-factor sign-in and passkeys protect you from thieves; recovery codes protect you from the ordinary mishaps of life — the dropped phone, the dead battery, the device that just stops working. Together they mean you get the strong protection without the fear of being locked out of your own life.

- A lost phone becomes an inconvenience, not a catastrophe.
- You can turn on strong protection without worrying it'll backfire.
- The people who help you have a clear path if something happens to you.

GOOD TO KNOW

The strongest security is the kind you'll actually keep turned on. Backup codes are what let you keep it on without fear, because they guarantee a way back in.

28. Putting it all together

The whole plan in one easy breath.

Let's bring it home. The heart of this guide fits in a sentence: when a service gives you backup codes, save them in two safe places — your password manager and a printed page — and add a backup phone or second method. Everything else here is detail around that one habit.

- 1 When you turn on 2FA or a passkey, save the codes before closing the screen.
- 2 Keep one copy in your password manager and one printed, in a safe spot.
- 3 Set a backup phone number and a recovery email, and keep them current.
- 4 Do a two-minute test so you know the routine.
- 5 Regenerate codes if you ever think the old set was seen.
- 6 Glance over it all once a year.

That's the whole thing. A small bit of care, done once, and your most important accounts have a spare key waiting — so a lost phone is a minor nuisance instead of a disaster.

GOOD TO KNOW

If any single step feels like one too many, you don't have to do it alone. Walking through exactly this, at your kitchen table or over a screen-share, is one of the most common things I help folks with.

CHEAT SHEET

Your Recovery-Codes Cheat Sheet

Keep this page by the computer. It's the short version of everything you need to find, save, and use your backup codes without panic.

Where each service keeps them (type these yourself)

- Google — myaccount.google.com, under Security, 2-Step Verification, 'Backup codes.'
- Apple — on your iPhone or iPad, Settings, your name, Sign-In & Security, 'Recovery Key.'

- Microsoft — account.microsoft.com, under Security, 'Advanced security,' recovery code.
- Password managers and other sites — look under Security or Two-Factor for 'recovery' or 'backup' codes.

When you first turn on 2FA or a passkey

- 1 Save the codes before you close the screen — they appear only once.
- 2 Store one copy in your password manager.
- 3 Print a copy and put it where you keep important papers.
- 4 Add a backup phone number or second method as well.

To use a code when you're locked out

- 1 At sign-in, choose 'Try another way' or 'Can't use your phone?'
- 2 Pick 'Enter a backup code' and type one in.
- 3 Each code works once — cross it off after you use it.

Good to keep in mind

- A password manager can hold the codes and your logins together.
- Generate fresh codes if you ever think the old list was seen.
- Test one code now so you know the routine before you need it.
- Stuck? Call Bill's Home Tech at (330) 200-8042.

WORDS TO KNOW

Plain-English Word List

Recovery codes — A short list of one-time codes a service gives you when you turn on extra sign-in protection. Each lets you in once if your usual method isn't available.

Backup codes — Another name for recovery codes. Same idea: spare keys for when your phone or app can't be used.

Two-factor (2FA) — A second step at sign-in beyond your password — a code, a tap, or a key — so a stolen password alone isn't enough.

Passkey — A newer sign-in that replaces the password with your phone or computer's own unlock, like Face ID or a fingerprint.

Recovery Key — Apple's name for a long backup code that locks down your Apple Account. Powerful, but if you lose it Apple can't get you back in.

Authenticator app — An app that makes the rotating six-digit codes used for two-factor sign-in. It lives on your phone.

Backup method — A second way to prove it's you — a spare phone number, a second email, or a trusted device — in case your first method fails.

Account recovery — The process a service puts you through to regain access when you've lost your password and your usual second step.

Password manager — A secure app that remembers your passwords, and can store recovery codes and notes, behind one master password.

One-time use — A code that stops working the moment it's used once. That's why a list is given, not a single code.

AT A GLANCE

A Picture to Follow Along

Save Your Codes the Moment You Get Them

The codes appear once, when you turn on 2FA or passkeys.



If you close that screen without saving, the codes are gone.

Illustration - recovery codes are shown once and rarely shown again.

AT A GLANCE

A Second Look

Good Places vs. Bad Places to Keep Codes

Where you store the codes decides whether they'll be there when you need them.

Good	Risky
- Your password manager - Printed, in a safe - A sealed envelope - Told to a trusted person	- A sticky note on screen - A plain text file named 'codes' - Only in your head - Only on the lost phone

Two safe copies beats one. One safe copy beats none.

Illustration - a code you can't find is the same as a code you never had.

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.