BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

Your Apple Account

Passwords, two-factor, recovery, family and purchases — keeping the key to your iPhone, iPad and Mac safe

A plain-English guide to the one account that runs it all

Take your time — you can't break it

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

For iPhone, iPad & Mac (iOS 26 & 27, recent macOS) · facts current November 2026

What's Inside

This is your Apple Account manual. Read it in any order and at your own pace — there is no test, and you can't fall behind. Parts 1 and 2 explain the account and your password. Parts 3 and 4 are the safety nets: two-factor, recovery contacts, legacy contacts and Stolen Device Protection. Part 5 covers family, subscriptions and money, and Part 6 shows you the scams aimed at your account. It's written for recent iPhones, iPads and Macs; if a screen looks a little different on yours, the idea is still the same.

Part 1 — Understanding Your Apple Account

1 A Note from Bill
2 What an Apple Account Is (and the Apple ID Rename)
3 What Your Apple Account Unlocks
4 Finding Your Account Screen

Part 2 — Your Password & Signing In

5 A Strong Password You Can Remember
6 Changing Your Password
7 Forgot Your Password? Your Three Ways Back In
8 Signing In on a New iPhone, iPad or Mac
9 Verification Codes: What They Are and Who Should See Them

Part 3 — Two-Factor Authentication & Trusted Devices

10 How Two-Factor Authentication Protects You
11 Trusted Phone Numbers
12 Your Device List: Who's Signed In
13 Security Keys (Optional, for the Extra Careful)

Part 4 — Planning for Lock-Outs, Theft & the Future

14 Recovery Contacts: A Trusted Person Who Can Help You Back In
15 The Recovery Key: Powerful, but Only If You Can Keep It Safe
16 Account Recovery & the Waiting Period
17 Legacy Contact: Planning Ahead for Your Family
18 Stolen Device Protection

Part 5 — Family, Purchases & Money

19 Family Sharing Basics
20 Ask to Buy: Approving a Child's Purchases
21 Subscriptions: Seeing and Canceling Them
22 Payment Methods: Your Card on File
23 Checking Charges & Asking for a Refund

Part 6 — Scams Aimed at Your Apple Account

24 Fake "Apple Support" Calls & Pop-Ups
25 Phishing Emails & Texts
26 Gift Card Scams
27 If You Think Someone Got Into Your Account

Part 7 — Your Check-Up, When to Call Bill & Your Cheat-Sheet

28 Your Once-a-Year Apple Account Check-Up
29 When to Call Bill
30 Your Apple Account Cheat-Sheet

PART 1

Understanding Your Apple Account

What an Apple Account is, why it matters so much, what changed when Apple renamed the Apple ID, and how to find your account screen on an iPhone, iPad or Mac.

CHAPTER 1

A Note from Bill

Hello, and welcome. Whoever is reading this guide, it's for **you**. Maybe you've been asked for an "Apple Account password" and you're not sure which password that is. Maybe a new iPhone is sitting in its box and you're nervous about setting it up. Or maybe you got a scary message that says your account has been locked. Wherever you're starting from, you're in the right place.

I'm Bill. With 30+ years of professional experience, I help folks here in Portage County, Ohio feel at home and safe with their technology. I wrote this guide the way I'd explain it sitting at your kitchen table: slowly, in plain English, one step at a time. Any word you might not know, I'll stop and explain right then.

Why this one account matters so much

Your **Apple Account** is the single key that unlocks your iPhone, your iPad, your Mac, your photos in iCloud, your apps, your music and your subscriptions. When it works, you barely notice it. When you're locked out of it, everything Apple you own can stop working at once. That's why a little planning now is worth so much later.

WHAT THIS DOES FOR YOU

What this guide does for you

By the end you'll know which password is your Apple Account password, how to change it safely, how to get back in if you forget it, and how to set up the backup plans (a recovery contact, a legacy contact and Stolen Device Protection) that keep a bad day from becoming a disaster. You'll also learn to spot the fake "Apple" calls and emails that try to steal your account.

The big promise: you can't break it

Looking at your account settings is completely safe. Opening a screen doesn't change anything. Apple asks you to confirm before anything important happens, usually with your passcode or Face ID. So take your time, look around and read each screen. Curiosity is how everyone learns.

And you're never stuck alone. If you'd like a hand, call me at **(330) 200-8042**. My help is $49 remote · $99 in your home, and there's no such thing as a silly question at my table.

— Bill

CHAPTER 2

What an Apple Account Is (and the Apple ID Rename)

An **Apple Account** is your personal membership with Apple. It's made of two things: an **email address** (or sometimes a phone number) that identifies you, and a **password** that proves it's really you. Everything you do with Apple, from buying an app to backing up your photos, is tied to that one account.

Apple ID is now called Apple Account

For many years Apple called this your **Apple ID**. In June 2024 Apple announced it was renaming it **Apple Account**, and the new name arrived with iOS 18, iPadOS 18 and macOS Sequoia in the fall of 2024. Nothing about your account changed. Same email, same password, same purchases. Only the name on the screen is different.

> GOOD TO KNOW
>
> **If someone says "Apple ID," they mean the same thing**
>
> Older articles, family members and even a few Apple web pages may still say Apple ID. Treat the two names as one and the same. You don't need to create anything new or "upgrade" your account.

Checked against Apple's June 2024 announcement as reported by MacRumors on November 13, 2026.

One account, not one per device

Most people should have **one** Apple Account and use it on every Apple device they own. Your iPhone, iPad and Mac then share the same photos, contacts, passwords and purchases. Two family members should each have their **own** account, then connect them with Family Sharing (*Family Sharing Basics* (Chapter 19)). Sharing one account between two people mixes up messages, contacts and photos.

Word you'll see	What it means
Apple Account	Your Apple membership: email + password. Formerly called Apple ID.
iCloud	Apple's online storage that uses your Apple Account to back up photos, contacts and more.
Passcode	The short number you type to unlock your iPhone or iPad. Not the same as your Apple Account password.

Word you'll see	What it means
Trusted device	An iPhone, iPad or Mac already signed in to your account, which can receive sign-in codes.
Trusted phone number	A phone number Apple can text or call with a sign-in code.

HEADS UP

Your passcode and your Apple Account password are different

This is the most common mix-up. Your **passcode** unlocks this one phone. Your **Apple Account password** is the password for your whole Apple membership. Write down which is which.

CHAPTER 3

What Your Apple Account Unlocks

It helps to know what's riding on this one account, so you understand why Apple protects it so carefully and why scammers want it so badly.

- **iCloud**: your photo library, contacts, calendars, notes and device backups.
- **Find My**: locating a lost iPhone, iPad, Mac, AirPods or AirTag, and locking or erasing a lost device.
- **The App Store**: every app you've bought or downloaded, and in-app purchases.
- **Subscriptions**: Apple Music, Apple TV, iCloud storage plans, Apple One and subscriptions you started inside apps.
- **Messages and FaceTime**: your iMessage and FaceTime identity.
- **Passwords**: the saved passwords for your other websites, kept in the Passwords app and iCloud Keychain.
- **Apple Pay and Apple Cash** settings on your devices.

WHAT THIS DOES FOR YOU

Why this matters to you

Because so much is connected, protecting this one account protects almost everything else. Ten minutes spent on the steps in Parts 3 and 4 of this guide does more for your safety than almost anything else you can do on an Apple device.

Activation Lock: why a lost iPhone stays useless to a thief

When **Find My** is on, your iPhone is tied to your Apple Account. Even if someone erases it, they can't set it up again without your Apple Account password. That's wonderful protection, and it's also why you must know your password before you sell, trade in or give away a device. More on that in *Your Once-a-Year Apple Account Check-Up* (Chapter 28).

TIP

Before you hand down an old iPhone

Sign out of your Apple Account on it first (that turns off Find My and Activation Lock), then erase it. If you skip the sign-out, the next owner will be stuck at a screen asking for *your* password.

CHAPTER 4

Finding Your Account Screen

Almost everything in this guide starts from one screen: your Apple Account screen. Here's how to reach it on each kind of device.

On an iPhone or iPad

1. Open **Settings** (the gray gear icon).
2. Tap **your name** at the very top of the list.
3. You're there. You'll see sections such as **Sign-In & Security**, **Payment & Shipping**, **Subscriptions**, **iCloud**, **Family Sharing** and **Find My**, and lower down, a list of your devices.

On a Mac

1. Click the **Apple menu** in the top-left corner of the screen.
2. Choose **System Settings**.
3. Click **your name** at the top of the sidebar.

On the web, from any computer

Go to **account.apple.com** and sign in. This is handy on a Windows PC, or when your Apple devices aren't nearby. Type the address yourself rather than clicking a link in an email.

Checked against Apple Support on November 13, 2026.

HEADS UP

Don't see your name at the top of Settings?

If Settings says **Sign in to your iPhone** (or **Apple Account**) instead of your name, this device isn't signed in. Tap it and sign in with your email and password, or see *Forgot Your Password? Your Three Ways Back In* (Chapter 7) if you've forgotten the password.

TIP

Write down your Apple Account email

Many people have more than one email address and aren't sure which one Apple uses. Your account email is shown right under your name on this screen. Write it in your password notebook now.

PART 2

Your Password & Signing In

A strong password you can actually remember, changing it safely, what to do when you forget it, and signing in on a new iPhone, iPad or Mac.

CHAPTER 5

A Strong Password You Can Remember

Your Apple Account password guards almost everything you own on Apple devices, so it deserves to be a good one. Good doesn't have to mean impossible to remember.

What makes a password strong

- **Long beats clever.** Three or four unrelated words strung together, with a number and a capital letter, is both strong and memorable.
- **Used nowhere else.** If your Apple password is the same as your email or shopping password, a break-in at any one of those sites puts your Apple Account at risk too.
- **Not about you.** Skip birthdays, pet names, street names and grandchildren's names. Those are the first things a scammer guesses.

TIP

A paper notebook is fine

Keeping your passwords in a notebook at home, away from the computer, is a perfectly sensible plan for most people. A thief across the world can't read a notebook in your kitchen drawer. Just don't keep it in your wallet or phone case.

Where to write it down

Write your Apple Account **email**, your **password**, your iPhone **passcode** and (if you make one) your **recovery key** on one page, and tell one trusted family member where that page lives. That single page has rescued more locked-out accounts than any setting.

STAY SAFE

Never give your password to a caller

Apple will never call, text or email asking for your Apple Account password or a verification code. Anyone who asks is a scammer, even if the caller ID says Apple. See *Fake "Apple Support" Calls & Pop-Ups* (Chapter 24).

CHAPTER 6

Changing Your Password

Change your password if you think someone else knows it, if you used it somewhere else, or if you simply want a better one. On a device you're already signed in to, it takes a minute.

On an iPhone or iPad

1. Open **Settings** and tap **your name**.
2. Tap **Sign-In & Security**.
3. Tap **Change Password**.
4. Enter your current password or your device **passcode** when asked.
5. Type a new password, type it again to confirm, then tap **Change**.

Checked against Apple Support on November 13, 2026.

On a Mac

1. Choose **Apple menu** > **System Settings**, then click **your name**.
2. Click **Sign-In & Security**, then **Change Password**.
3. Enter the password you use to unlock your Mac, then type and confirm the new password.

On the web

Go to **account.apple.com**, sign in, choose **Sign-In and Security**, then **Password**.

Checked against Apple Support on November 13, 2026.

GOOD TO KNOW

Asked to wait an hour?

If **Stolen Device Protection** is on and you're away from home or work, your iPhone may make you wait about an hour before it lets you change your Apple Account password. That's on purpose: a thief who learned your passcode can't lock you out in a hurry. See *Stolen Device Protection* (Chapter 18).

HEADS UP

Your other devices will ask for the new password

After a change, your other iPhone, iPad, Mac or Apple TV may pop up a request to sign in again. That's normal. Type the new password on each one.

CHAPTER 7

Forgot Your Password? Your Three Ways Back In

Forgetting your Apple Account password is common and usually very fixable. Apple gives you three routes. Try them in this order.

Way 1: Use your own iPhone, iPad or Mac (easiest)

If you still have a device that's signed in to your account and has a passcode, you can reset the password without knowing the old one. Your passcode proves it's you.

1. Open **Settings** and tap **your name**.
2. Tap **Sign-In & Security**, then **Change Password**.
3. Enter your iPhone **passcode**.
4. Type a new password twice and tap **Change**.

Way 2: Borrow a family member's iPhone or iPad

1. On their device, open the **Apple Support** app (it's free in the App Store).
2. Scroll down to **Support Tools** and tap **Reset Password**.
3. Choose **Help Someone Else**.
4. Enter *your* Apple Account email or phone number and follow the steps. Apple says the information you type isn't stored on the borrowed device.

Way 3: On the web

From any web browser, type **iforgot.apple.com** and follow the steps. You'll usually confirm a code sent to your trusted phone number.

Checked against Apple Support on November 13, 2026.

GOOD TO KNOW

Setting up a new device and stuck at the sign-in screen?

On the Apple Account sign-in screen during setup, tap **Forgot password or don't have an Apple Account?** and follow the steps.

HEADS UP

If none of these work

If you can't reset the password with any of the three ways, Apple has a slower, safer process called **account recovery**. It can take days. That's covered in *Account Recovery & the Waiting Period* (Chapter 16), and it's exactly why a recovery contact (*Recovery Contacts: A Trusted Person Who Can Help You Back In* (Chapter 14)) is worth setting up today.

SCAM ALERT

There is no paid "Apple unlock service"

Websites and callers that charge to "unlock" or "recover" your Apple Account are scams. Apple's own reset tools are free and are the only real way in.

CHAPTER 8

Signing In on a New iPhone, iPad or Mac

When you set up a new device, it will ask you to sign in with your Apple Account. This is the moment that brings your photos, contacts, messages and apps onto the new device, so it's worth getting right.

Have these ready before you start

- Your Apple Account **email** and **password**.
- Your **old iPhone** nearby and charged, if you have one. It can receive the sign-in code and transfer your things.
- Your **Wi-Fi password**.
- An hour of unhurried time. New-phone setup goes better when no one is rushing.

What happens during sign-in

1. Enter your Apple Account email and password on the new device.
2. A message appears on your old iPhone (or another trusted device) saying someone is signing in, often with a map of roughly where.
3. If it's you, tap **Allow**. A six-digit **verification code** appears.
4. Type that code on the new device. You're in.

GOOD TO KNOW

No old device nearby?

On the new device, tap **Didn't get a verification code?** and choose one of your trusted phone numbers. Apple will text or call that number with the code. This is one reason to keep a second number, such as your home phone, on file (*Trusted Phone Numbers* (Chapter 11)).

Checked against Apple Support on November 13, 2026.

HEADS UP

The map may look wrong

The location on the sign-in message is a rough guess based on the internet connection, and it can show a nearby town. What matters is whether *you* are the one signing in right now.

STAY SAFE

Tap Don't Allow if it isn't you

If a sign-in request appears and you're not setting anything up, tap **Don't Allow**. Then change your password (*Changing Your Password* (Chapter 6)). Never read the code to anyone.

CHAPTER 9

Verification Codes: What They Are and Who Should See Them

A **verification code** is a six-digit number Apple shows on your trusted device, or sends to your trusted phone number, when you sign in somewhere new. It's a one-time key that proves you're the one signing in.

The one rule

The only place a verification code ever goes is the screen of the device you are personally setting up. Not to a caller, not into a text reply, not to a website someone sent you to.

SCAM ALERT

"Read me the code we just sent you"

This is one of the most common account-stealing tricks. A caller pretending to be Apple, your bank or a delivery company says they're "verifying" you and asks for the code that just arrived. In truth they're signing in to *your* account on their device, and the code is the last thing they need. Hang up.

Getting a code when you need one

- **Automatic:** it pops up on your other signed-in devices when you sign in somewhere new.
- **By text or call:** tap **Didn't get a verification code?** on the device you're signing in to.

TIP

Got a code you didn't ask for?

Ignore it and don't share it. On its own a code is harmless. It means someone typed your email and password somewhere, so it's a good moment to change your password.

PART 3

Two-Factor Authentication & Trusted Devices

The second lock on your account: how two-factor works, keeping your trusted phone numbers current, checking which devices are signed in, and optional security keys.

CHAPTER 10

How Two-Factor Authentication Protects You

Two-factor authentication means signing in takes two things: something you *know* (your password) and something you *have* (your iPhone, or your phone number). A thief who steals or guesses your password still can't get in without the second piece.

WHAT THIS DOES FOR YOU

Why this helps you

Most account break-ins start with a stolen or reused password. With two-factor on, a password alone isn't enough. It's one of the biggest safety upgrades there is, and on a current Apple Account it's already working for you.

Is it on for me?

1. Open **Settings** and tap **your name**.
2. Tap **Sign-In & Security**.
3. Look at **Two-Factor Authentication**. It should say **On**.

Accounts created on recent Apple devices have two-factor turned on from the start, and several Apple features, including recovery contacts and legacy contacts, require it.

Checked against Apple Support on November 13, 2026.

What it looks like day to day

Mostly, nothing. On devices you already use, you won't be asked for codes. You'll only see the second step when you sign in on a **new** device or browser, or after you change your password.

GOOD TO KNOW

Don't let anyone talk you into turning it off

Apple doesn't ask customers to turn off two-factor authentication. If someone on the phone suggests it to "fix" a problem, that's a red flag.

CHAPTER 11

Trusted Phone Numbers

A **trusted phone number** is a number Apple can text or call with a verification code. You need at least one. Having two is much safer, because if you lose your cell phone you can still get a code on the other.

Add a second number

1. Open **Settings** and tap **your name**.
2. Tap **Sign-In & Security**, then **Two-Factor Authentication**.
3. Tap **Add a Trusted Phone Number**. You may be asked for your passcode.
4. Type the number and choose whether Apple should send a **text message** or make a **phone call**.
5. Enter the code Apple sends to that number to confirm it.

Checked against Apple Support on November 13, 2026.

> **TIP**
> **A home phone or a family member's cell makes a good second number**
> Apple suggests verifying other numbers you can reach, such as a home phone. A landline that can receive a **phone call** works well. A grown child's cell phone is another option if you trust them and they live nearby.

Remove an old number

On the same **Two-Factor Authentication** screen, tap **Edit** and remove a number you no longer have. Apple won't let you remove your only trusted number, so add the new one first.

On the web or a Mac

On a Mac: **System Settings** > **your name** > **Sign-In & Security** > **Two-Factor Authentication**. On the web: sign in at **account.apple.com** and go to **Sign-In and Security** > **Account Security**.

Checked against Apple Support on November 13, 2026.

HEADS UP

Changing cell carriers or numbers?

Add your new number *before* the old one stops working. People who change numbers and forget this step are some of the most common lock-outs.

CHAPTER 12

Your Device List: Who's Signed In

Your account keeps a list of every device signed in to it. Checking it now and then is a quick way to spot an old phone you forgot about, or a device you don't recognize.

See the list

1. Open **Settings** and tap **your name**.
2. Scroll down. Below the settings you'll see each device signed in, such as "Mary's iPhone" or "iMac."
3. Tap any device to see its model and details.

Remove a device you no longer use

1. Tap the device in the list.
2. Tap **Remove from Account** and confirm.

A removed device can no longer use iCloud or Find My on your account, and it stops receiving your verification codes. If that device is still signed in somewhere, it can reappear the next time it connects to the internet, so also sign out on the device itself if you can.

Checked against Apple Support on November 13, 2026.

TIP

From a Mac or a Windows PC

On a Mac: **System Settings** > **your name**, then scroll down. From any computer: sign in at **account.apple.com** and choose **Devices**.

STAY SAFE

See a device you don't recognize?

Remove it, then change your password right away (*Changing Your Password* (Chapter 6)). Removing it alone isn't enough, because whoever has your password could sign in again.

GOOD TO KNOW

A separate list for purchases

Apple also keeps a list of devices allowed to download your music and video purchases. That one is managed under **Media & Purchases** on iPhone or iPad. You'll rarely need it.

CHAPTER 13

Security Keys (Optional, for the Extra Careful)

A **security key** is a small physical gadget, a little like a house key, that plugs into or taps against your device. With security keys turned on, signing in on a new device requires the key instead of a six-digit code. It makes the "read me the code" scam impossible.

Is it for you?

- **Probably not** for most people. If you lose the keys and your devices, getting back in is harder.
- **Worth considering** if you've been targeted repeatedly, handle a family's finances online, or simply want the strongest protection and are organized about keeping things safe.

What you need

- At least **two** keys (Apple requires two, and allows up to six). Keep one at home and one somewhere safe.
- Keys that are **FIDO Certified** and have a connector that fits your devices (for example USB-C, or NFC to tap on an iPhone).
- A passcode on the device you use to add them.

Adding keys on an iPhone

1. Open **Settings** > **your name** > **Sign-In & Security**.
2. Tap **Two-Factor Authentication**, then **Security Keys**.
3. Tap **Add Security Keys** and follow the steps for each key.

Checked against Apple Support on November 13, 2026.

FROM BILL

Want a second opinion first?

Security keys are excellent, but they're a commitment. If you're thinking about them, I'm happy to talk it through and set them up with you. $49 remote · $99 in your home.

PART 4

Planning for Lock-Outs, Theft & the Future

The backup plans that turn a bad day into a small hiccup: recovery contacts, recovery keys, Apple's account recovery wait, legacy contacts and Stolen Device Protection.

CHAPTER 14

Recovery Contacts: A Trusted Person Who Can Help You Back In

A **recovery contact** is someone you trust, such as a son, daughter or close friend with an iPhone, who can help you get back into your account if you ever forget your password or get locked out. They can't see your photos, messages or anything else. All they can do is show you a code that proves it's really you.

WHAT THIS DOES FOR YOU

Why this helps you

Without a recovery contact, a forgotten password with no trusted device can mean Apple's account-recovery wait, which can stretch for days. With one, a quick phone call to your daughter and a code from her iPhone can have you back in within minutes.

What you both need

- **Two-factor authentication** turned on for your account (*How Two-Factor Authentication Protects You* (Chapter 10)).
- **iMessage** turned on for both of you.
- Your contact must be **over 13**, have an Apple device on iOS 15, iPadOS 15 or macOS 12 or later, with two-factor on and a passcode set.

Set one up on your iPhone

1. Open **Settings** and tap **your name**.
2. Tap **Sign-In & Security**, then **Recovery Contacts**. (On some versions this is under **Account Recovery**.)
3. Tap **Add Recovery Contact** and confirm with Face ID, Touch ID or your passcode.
4. Choose the person from your contacts. Apple sends them a message explaining what it means.
5. Once they accept, you'll see them listed as your recovery contact.

Checked against Apple Support on November 13, 2026.

If you're ever locked out

1. Call or visit your recovery contact.

2. On their iPhone they go to **Settings** > **their name** > **Sign-In & Security** > **Recovery Contacts**, tap your name, and get a recovery code.
3. You type that code on your device when it asks, then set a new password.

STAY SAFE

Only accept codes from the person themselves

A real recovery code comes from your own family member, in person or on a call you placed to them. No one from "Apple" will ever call offering to be your recovery contact or to give you a code.

CHAPTER 15

The Recovery Key: Powerful, but Only If You Can Keep It Safe

A **recovery key** is a secret 28-character code that you create and keep. Along with a trusted phone number and an Apple device, it can be used to get back into your account and reset your password.

HEADS UP

Most people should skip this one

A recovery key puts *you* in charge of your own rescue. If you turn one on and later lose both the key and access to your trusted devices, getting back in may not be possible. For most households, a **recovery contact** (*Recovery Contacts: A Trusted Person Who Can Help You Back In* (Chapter 14)) is the friendlier choice.

If you decide to make one

1. Open **Settings** > **your name** > **Sign-In & Security**.
2. Tap **Recovery Key** and turn it on. Confirm with your passcode.
3. Write the 28 characters down carefully, exactly as shown. Print it too if you can.
4. Type it back in when asked, to confirm you copied it correctly.
5. Store the paper somewhere safe and lasting, such as a fireproof box, and tell a trusted family member where it is.

On a Mac, the same option is in **System Settings** > **your name** > **Sign-In & Security** > **Recovery Key**.

Checked against Apple Support on November 13, 2026.

Lost the paper?

If you still have a trusted device, go back to the same **Recovery Key** screen and tap **Replace Recovery Key** to make a new one. The old key stops working.

Checked against Apple Support on November 13, 2026.

CHAPTER 16

Account Recovery & the Waiting Period

If you use two-factor authentication and can't sign in or reset your password any of the usual ways, Apple offers **account recovery**. It's the last resort, and it's deliberately slow: Apple makes you wait so a stranger can't take over your account just by claiming to be you.

Starting account recovery

1. Go to **iforgot.apple.com**, or start from **Forgot password** on an Apple device sign-in screen.
2. Enter your Apple Account email and follow the steps. Give as much information as you can.
3. Apple tells you when to expect a text or call with next steps.
4. When the waiting period ends, Apple contacts your trusted number with instructions. If the text or call doesn't come, you can go straight back to **iforgot.apple.com**.

Checked against Apple Support on November 13, 2026.

GOOD TO KNOW

How long is the wait?

Apple doesn't publish a fixed time, and it varies from account to account. It can be a few days or longer. Apple Support can't speed it up, so don't pay anyone who claims they can.

Things to know while you wait

- **If you remember your password** and sign in successfully, the wait cancels automatically and your account works right away.
- **Keep your trusted phone** with you and charged; that's where Apple's message will arrive.

SCAM ALERT

Callers who offer to "speed up" recovery are scammers

Real account recovery happens only through Apple's own pages and messages. Anyone offering to shorten the wait, for a fee or for your codes, is trying to steal the account.

TIP

The best way to avoid the wait

Set up a **recovery contact** (*Recovery Contacts: A Trusted Person Who Can Help You Back In* (Chapter 14)) and a **second trusted number** (*Trusted Phone Numbers* (Chapter 11)) today. Then account recovery becomes something you'll probably never need.

CHAPTER 17

Legacy Contact: Planning Ahead for Your Family

A **Legacy Contact** is someone you choose who can request access to the data in your Apple Account after you pass away: your photos, notes, files and more. Without one, even a spouse or child can find it very hard to get at family photos stored in iCloud.

WHAT THIS DOES FOR YOU

Why this matters

It's a kindness to the people you love. For many families, a parent's iCloud photos are a treasured record of decades. Five minutes now saves them a long, painful process later.

What you need

- An Apple device running iOS 15.2, iPadOS 15.2 or macOS Monterey 12.1 or later, signed in to your account.
- **Two-factor authentication** turned on.

Add a Legacy Contact on your iPhone

1. Open **Settings** > **your name** > **Sign-In & Security**.
2. Tap **Legacy Contact**, then **Add Legacy Contact**, and confirm with your passcode or Face ID.
3. Choose the person.
4. Decide how to share the **access key**. If they have an Apple device, you can send it by iMessage, and their device stores it in their account settings. You can also print a copy.

Checked against Apple Support on November 13, 2026.

What your Legacy Contact will need later

- The **access key**.
- A copy of your **death certificate**.
- They make the request through Apple, and Apple reviews it before granting access.

HEADS UP

Keep the access key safe

Apple can't look up or replace a lost access key. If you print it, keep it with your will or other important papers. If you name more than one Legacy Contact, any one of them can make decisions about your data, including deleting it, so choose people who will agree.

Checked against Apple Support on November 13, 2026.

CHAPTER 18

Stolen Device Protection

Thieves sometimes watch over someone's shoulder to learn their iPhone passcode, then steal the phone. With the passcode alone they used to be able to change the Apple Account password and lock the owner out. **Stolen Device Protection** stops that.

What it does

- When your iPhone is **away from familiar places** like home or work, certain sensitive actions need **Face ID or Touch ID**, not just the passcode.
- The most important changes, such as changing your Apple Account password, also come with a **security delay** of about an hour before you can make them.
- At home or work, your iPhone works the way it always has, unless you choose stronger settings.

WHAT THIS DOES FOR YOU

Why this helps you

Even if a thief learns your passcode, they can't quickly change your password, turn off Find My or take over your account. That hour gives you time to mark the phone as lost and protect yourself.

Turn it on

1. Open **Settings**.
2. Tap **Face ID & Passcode** (or **Touch ID & Passcode**) and enter your passcode.
3. Tap **Stolen Device Protection** and turn it on.
4. Optional: under **Require Security Delay**, choose **Always** if you'd like the delay even at home.

Checked against Apple Support on November 13, 2026.

GOOD TO KNOW

Asked to wait even though you're home?

Your iPhone learns familiar places over time. After you restore from a backup or move to a new iPhone, it may take a while to recognize home again. The delay can also end early once your iPhone sees you've arrived somewhere familiar.

HEADS UP

Turn it off before you sell or trade in

Apple recommends turning Stolen Device Protection off before you sell, give away or trade in your iPhone. If you're away from a familiar place when you try, the security delay starts first, so do it at home.

Checked against Apple Support on November 13, 2026.

PART 5

Family, Purchases & Money

Family Sharing, approving a grandchild's purchases, finding and canceling subscriptions, updating your card on file, and checking or disputing charges.

CHAPTER 19

Family Sharing Basics

Family Sharing lets up to six people, each with their own Apple Account, share things like app purchases, an Apple subscription, iCloud storage and locations, without sharing passwords.

How it's organized

- One adult is the **organizer**. The organizer starts the family group, chooses what's shared and invites up to five other people.
- Everyone keeps their **own** Apple Account, password, messages and photos.
- A person can belong to only **one** family group at a time.

Start a family group

1. Open **Settings** and tap **your name**.
2. Tap **Family Sharing**.
3. Follow the onscreen steps to set up your family and invite members. They receive an invitation they can accept on their own device.
4. Tap any feature, such as **Purchase Sharing** or **Location Sharing**, to choose what your family shares.

Checked against Apple Support on November 13, 2026.

WHAT THIS DOES FOR YOU

Why this helps

One iCloud storage plan or Apple One subscription can cover the whole family, which often costs less than separate plans. Family members can also see each other's location in Find My, which is a real comfort if someone has a fall or gets lost.

HEADS UP

Purchase Sharing means one card pays

When the organizer turns on **Purchase Sharing**, purchases made by family members are generally charged to the organizer's payment method. That's convenient, but it's worth knowing before you invite a grandchild who likes games.

CHAPTER 20

Ask to Buy: Approving a Child's Purchases

Ask to Buy means a child in your family group has to ask before buying or downloading something. The request pops up on the organizer's (or a parent's) device, and you tap to approve or decline.

Turn it on

1. Open **Settings** and tap **Family**.
2. Tap the child's name.
3. Find **Ask to Buy** and turn on **Require Purchase Approval**.

Checked against Apple Support on November 13, 2026.

TIP

Missed a request?

If you dismiss the notification by accident, the request also appears in **Messages**, so you can still approve or decline it there.

GOOD TO KNOW

Age rules vary

Ask to Buy is for children in your family group. The ages it applies to depend on your country. Only the organizer, or a parent or guardian in the group, can turn it on.

FROM BILL

Grandparents set up Family Sharing too

If you'd like to be part of your children's family group, or start one with your spouse, I'm glad to help sort out who should be the organizer and what to share. $49 remote · $99 in your home.

CHAPTER 21

Subscriptions: Seeing and Canceling Them

A **subscription** is anything that charges you again and again: Apple Music, extra iCloud storage, a streaming service you signed up for inside an app, a game's monthly pass. It's easy to forget a free trial that turned into a paid plan. Your iPhone shows them all in one list.

See every subscription

1. Open **Settings** and tap **your name**.
2. Tap **Subscriptions**.
3. You'll see your **Active** subscriptions, with their price and renewal date, and below them your **Expired** ones.

Cancel one

1. Tap the subscription in the list.
2. Tap **Cancel Subscription**. You may need to scroll down to see it.
3. Confirm. You can usually keep using it until the end of the period you've already paid for.

Checked against Apple Support on November 13, 2026.

GOOD TO KNOW

No Cancel button?

If there's no Cancel button, or you see an expiration date in red, that subscription is already canceled and won't charge you again.

HEADS UP

Not on the list?

If a charge doesn't appear here, it was probably billed by another company, not Apple. Check your bank or card statement for the company's name, then cancel with them directly. And a family member's subscription can only be canceled by that family member.

On a Mac

Open the **App Store**, click **your name**, then **Account Settings**, and find **Subscriptions**.

Checked against Apple Support on November 13, 2026.

TIP

Make it a habit

Look at this list every few months, perhaps when the seasons change. It takes a minute and often turns up a forgotten trial.

CHAPTER 22

Payment Methods: Your Card on File

Your Apple Account keeps a payment method, usually a credit or debit card, for App Store purchases and subscriptions. When a card expires or is replaced after fraud, you'll need to update it here, or your subscriptions may stop.

Update or change your card

1. Open **Settings** and tap **your name**.
2. Tap **Payment & Shipping**. You may be asked to sign in.
3. To update a card that's already there, tap it, then tap **Edit**, enter the new details and tap **Done**.
4. To use a different card, add the new payment method first.
5. Then tap **Edit**, tap the red delete button next to the old card and tap **Remove**.

Checked against Apple Support on November 13, 2026.

GOOD TO KNOW

Can't remove a card?

If you have an active subscription or an unpaid balance, Apple may need at least one payment method on file. Change it instead of removing it. You can also manage payment methods by signing in at **account.apple.com**.

SCAM ALERT

"Your payment failed, update your billing"

Fake emails and texts claiming your Apple payment failed are common. They link to a copycat page that steals your card. Never tap the link. Instead, open **Settings** > **your name** > **Payment & Shipping** yourself. If there's really a problem, you'll see it there.

CHAPTER 23

Checking Charges & Asking for a Refund

If you see a charge on your card from "Apple.com/bill" and aren't sure what it is, you can look it up yourself before calling anyone.

Look up a charge

1. On any web browser, type **reportaproblem.apple.com** and sign in with your Apple Account.
2. You'll see your recent purchases and subscription charges with dates and prices.
3. Match the charge on your statement to an item in the list.

GOOD TO KNOW

Still can't find it?

Make sure you're signed in with the same Apple Account that made the purchase. And check whether a family member in your Family Sharing group bought it with your card.

Ask for a refund

1. At **reportaproblem.apple.com**, choose **I'd like to** and pick **Request a refund**.
2. Choose the reason and the item, then submit.
3. Come back to the same site later to check the status of your request.

Refunds aren't guaranteed, and if Apple approves one, it can take a little while for the money to show up back on your card. To stop a subscription from charging again, cancel it (*Subscriptions: Seeing and Canceling Them* (Chapter 21)).

Checked against Apple Support on November 13, 2026.

SCAM ALERT

Fake "Apple receipt" emails

A common trick is a fake receipt for something expensive you never bought, with a phone number to "dispute" it. The number reaches a scammer. Check your real purchases at **reportaproblem.apple.com** instead, typed in by hand.

PART 6

Scams Aimed at Your Apple Account

Fake Apple support calls, phishing emails and texts, gift card demands, and exactly what to do if you think someone got into your account.

CHAPTER 24

Fake "Apple Support" Calls & Pop-Ups

Some of the most convincing scams pretend to come from Apple itself. The caller ID may even say "Apple Inc." The voice is polite and urgent: your account has been hacked, your iCloud was breached, someone in another state is using your Apple Pay.

What Apple says to do

Apple's own advice is simple: don't answer suspicious calls or messages claiming to be from Apple. Instead, contact Apple directly through its official support channels.

Checked against Apple Support on November 13, 2026.

Signs it's a scam

- They called **you**, out of the blue, about a problem you didn't know you had.
- They want your **password**, a **verification code** or your **passcode**.
- They want you to install an app so they can "see your screen" or "fix" your device.
- They want payment by **gift card**, wire transfer, cryptocurrency or a payment app.
- They say you must act **right now** and not tell anyone.

SCAM ALERT

Hang up, then call Apple yourself

If you're worried, hang up and call Apple at the number you look up yourself: in the U.S., **1-800-275-2273**, or use the free **Apple Support** app. Never call back a number given to you by the caller, a text or a pop-up.

Pop-ups that say your iPhone or Mac is infected

A web page that suddenly fills the screen with warnings, beeping or a countdown, and gives a phone number for "Apple Support," is a scam. Close the browser tab or quit the browser. On an iPhone, swipe up from the bottom and swipe Safari away. Don't call the number.

TIP

Want a quick second opinion?

If you're ever unsure whether a call or message is really Apple, call me at **(330) 200-8042** before you do anything. I'd always rather hear from you first.

CHAPTER 25

Phishing Emails & Texts

Phishing is a fake message designed to get you to tap a link and type your Apple Account password into a copycat page. They look remarkably real, with Apple's logo, colors and wording.

Common examples

- "Your Apple Account has been locked for security reasons. Verify now."
- "Your iCloud storage is full. Your photos will be deleted."
- "Your payment method was declined. Update your billing information."
- "Receipt: you purchased ..." for something you never bought, with a number to call.

The safe habit

Never use the link in the message. Instead, open **Settings** on your iPhone, tap your name, and look for yourself. If there's a real problem with your account, password or payment method, it shows up there. Or type **account.apple.com** into your browser by hand.

Report it to Apple

- **Suspicious email:** forward it to **reportphishing@apple.com**.
- **Suspicious text:** take a screenshot and email it to **reportphishing@apple.com**.
- **Suspicious iMessage:** tap **Report Junk** under the message.

Apple reads these reports but may not reply. Then delete the message.

Checked against Apple Support on November 13, 2026.

STAY SAFE

Already typed your password into a fake page?

Don't panic. Change your Apple Account password right away from **Settings** (*Changing Your Password* (Chapter 6)), then work through *If You Think Someone Got Into Your Account* (Chapter 27). Acting quickly makes a big difference.

CHAPTER 26

Gift Card Scams

Apple Gift Cards are a favorite tool of scammers, because once you read someone the code on the back, the money can be spent in moments and is very hard to get back.

The one thing to remember

Apple Gift Cards can be used only to buy products and services from Apple. No government office, utility, hospital, bail bond company, debt collector or tech-support line will ever ask you to pay with one. If anyone asks you to buy Apple Gift Cards and read them the numbers, it's a scam, every single time.

What the scam sounds like

- "You owe back taxes and must pay today."
- "Your grandson is in jail and needs bail."
- "Your power will be shut off in an hour."
- "We refunded you too much; send the difference back in gift cards."

SCAM ALERT

If you've already shared a gift card code

Apple says the money on a card may be spent before you can reach anyone, so act fast. In the U.S., call Apple at **1-800-275-2273** and say "gift cards" when prompted. Keep the card and your receipt. Then report the scam to the FTC at **ReportFraud.ftc.gov**.

Checked against Apple Support on November 13, 2026.

TIP

A note for store clerks and families

If an older relative suddenly wants to buy several gift cards and seems rushed or secretive, gently ask who asked them to. That one question stops many of these scams.

CHAPTER 27

If You Think Someone Got Into Your Account

Signs someone else may be using your account: emails from Apple about changes you didn't make, a device in your list you don't recognize, purchases you didn't make, or your password suddenly not working. Here's what to do, in order.

1. **Change your password** right away from a device you're signed in to (*Changing Your Password* (Chapter 6)). If you can't sign in, use **iforgot.apple.com** (*Forgot Your Password? Your Three Ways Back In* (Chapter 7)).
2. **Check your device list** and remove anything you don't recognize (*Your Device List: Who's Signed In* (Chapter 12)).
3. **Check your trusted phone numbers** and remove any you don't recognize (*Trusted Phone Numbers* (Chapter 11)).
4. **Check your email address and contact details** on the account screen and fix anything that was changed.
5. **Look at recent purchases** at **reportaproblem.apple.com** (*Checking Charges & Asking for a Refund* (Chapter 23)).
6. **Check Payment & Shipping** and call your card company if there are charges you didn't make.
7. **Change the password on your email account**, too, if your Apple Account uses that email. Whoever controls your email can often reset other passwords.

HEADS UP

Locked out completely?

If the password was changed and none of the reset routes work, use account recovery (*Account Recovery & the Waiting Period* (Chapter 16)) or ask your recovery contact for a code (*Recovery Contacts: A Trusted Person Who Can Help You Back In* (Chapter 14)). Contact Apple through the Apple Support app or by calling **1-800-275-2273**.

FROM BILL

This is a good time to call me

If you think your account was taken over, you don't have to sort it out alone. I'll go through each step with you and make sure the door is locked behind us. Call **(330) 200-8042**. $49 remote · $99 in your home.

PART 7

Your Check-Up, When to Call Bill & Your Cheat-Sheet

A once-a-year account check-up, what to do before selling or handing down a device, when to pick up the phone, and a one-page summary to keep.

CHAPTER 28

Your Once-a-Year Apple Account Check-Up

Pick a date you'll remember, such as your birthday or New Year's Day, and spend fifteen minutes on this list. It keeps everything current so you never get surprised.

Check	Where	What you're looking for
Your password	Settings > your name > Sign-In & Security	Still strong, still written down, used nowhere else.
Two-factor	Sign-In & Security	Says On.
Trusted numbers	Sign-In & Security > Two-Factor Authentication	At least two, both still yours.
Recovery contact	Sign-In & Security > Recovery Contacts	Someone you still trust and can reach.
Legacy Contact	Sign-In & Security > Legacy Contact	Set up, and the access key stored safely.
Device list	Settings > your name, scroll down	Only devices you own and use.
Subscriptions	Settings > your name > Subscriptions	Nothing you've forgotten or don't want.
Payment method	Settings > your name > Payment & Shipping	Current card, not expired.
Stolen Device Protection	Settings > Face ID & Passcode	Turned on.

Before you sell, trade in or hand down a device

1. Turn off **Stolen Device Protection** while you're at home (*Stolen Device Protection* (Chapter 18)).
2. Make sure your things are backed up to iCloud or your new device.
3. Sign out of your Apple Account on the old device: **Settings** > **your name**, scroll to the bottom and tap **Sign Out**. This turns off Find My and Activation Lock.
4. Erase the device: **Settings** > **General** > **Transfer or Reset iPhone** > **Erase All Content and Settings**.
5. Check your device list from another device and remove the old one if it's still there (*Your Device List: Who's Signed In* (Chapter 12)).

GOOD TO KNOW

Family members inheriting your old iPhone

Once it's erased, they set it up with **their own** Apple Account, not yours. That keeps your messages and photos private and theirs separate.

CHAPTER 29

When to Call Bill

This guide is here to make you confident with your Apple Account. But the smartest people aren't the ones who never ask for help; they're the ones who ask before a small problem becomes a big one. Here's when I'd want you to pick up the phone.

Call me when

- **You're locked out** and the reset steps in *Forgot Your Password? Your Three Ways Back In* (Chapter 7) aren't working.
- **You got a call, email or text "from Apple"** and you're not sure it's real.
- **You read someone a code or a password**, or let a caller onto your device.
- **You'd like the backup plans set up**: recovery contact, legacy contact, a second trusted number, Stolen Device Protection.
- **You're getting a new iPhone** and want your photos, contacts and messages moved over safely.
- **You're helping a parent** whose Apple Account is in a muddle, or who uses two accounts by mistake.

FROM BILL

How I like to help

I'm Bill, and with 30+ years of professional experience, I help folks feel at home and safe with their technology, right here in Portage County, Ohio. I don't rush, and I don't talk down to anyone. Whether it's a quick "is this real?" call or sitting down together to set up every safety net in this guide, we'll handle it together. $49 remote · $99 in your home. Call **(330) 200-8042** or book a time at **billshometech.com/book**. If I can't get to the phone, Sophie, my AI receptionist, will answer.

STAY SAFE

I'll never ask for your password over the phone

If we work together remotely, you stay in control of your own screen and type your own passwords. Anyone claiming to be me who asks for your Apple Account password or codes is not me.

Thank you for taking the time to learn this. Your Apple Account is the front door to so much of your digital life, and you now know how to keep it locked, how to get back in, and how to

spot the people pretending to be Apple. That's something to be proud of.

— Bill

CHAPTER 30

Your Apple Account Cheat-Sheet

Copy the important parts of this onto a card and keep it with your password notebook.

Where things are (iPhone)

To do this	Go here
See your account	Settings > your name
Change password	Settings > your name > Sign-In & Security > Change Password
Trusted numbers	Settings > your name > Sign-In & Security > Two-Factor Authentication
Recovery contact	Settings > your name > Sign-In & Security > Recovery Contacts
Legacy Contact	Settings > your name > Sign-In & Security > Legacy Contact
Subscriptions	Settings > your name > Subscriptions
Card on file	Settings > your name > Payment & Shipping
Stolen Device Protection	Settings > Face ID & Passcode > Stolen Device Protection

Web addresses to type by hand

- **account.apple.com**: manage your account from any computer.
- **iforgot.apple.com**: reset a forgotten password or start account recovery.
- **reportaproblem.apple.com**: see purchases and ask for refunds.
- **reportphishing@apple.com**: forward fake Apple emails.

Bill's golden rules

- **Never** read a verification code, password or passcode to anyone.
- **Never** pay anyone with Apple Gift Cards. They're only for buying from Apple.
- **Never** tap links in "Apple" emails or texts. Open Settings and look yourself.
- **Hang up** on callers claiming to be Apple. Call Apple yourself if you're worried.
- **Keep two trusted phone numbers** and a recovery contact.
- **When in doubt, call someone you trust** before you act.

Numbers to keep

- **Apple Support (U.S.):** 1-800-275-2273, or the Apple Support app.
- **Report fraud:** ReportFraud.ftc.gov

- **Bill's Home Tech:** (330) 200-8042 · billshometech.com/book

Checked against Apple Support on November 13, 2026.

Bill's Home Tech · Complete Manuals Series · (330) 200-8042 · billshometech.com · Portage County, Ohio