BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

Authenticator Apps & Passkeys

Codes, sign-in prompts, passkeys and backup codes — explained in plain English, one step at a time

A plain-English guide to the second lock on your accounts

Take your time — and always keep a spare way in

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

For iPhone, Android, Windows & Mac · Google, Microsoft, Apple, Amazon & PayPal · facts current November 2026

What's Inside

This is your guide to the "second lock" on your online accounts: the codes, the tap-to-approve prompts, and the new passkeys that are replacing passwords. Start with Part 1, then turn to whatever you need. Read in any order and at your own pace. If a screen looks a little different on your phone or computer, the idea is still the same.

Part 1 — The Big Picture

1 A Note from Bill
2 What Two-Step Verification Is
3 Text Codes, Apps, Prompts, Passkeys and Keys
4 What a Passkey Really Is
5 Your One-Hour Safety Plan

Part 2 — Authenticator Apps & Sign-In Prompts

6 How Authenticator Apps Work
7 Google Authenticator: Getting Started
8 Adding a Website to Your Authenticator App
9 Google Authenticator Backup: Sync with Your Google Account
10 Microsoft Authenticator: Getting Started
11 Approving Sign-Ins with Microsoft Authenticator
12 Microsoft Authenticator's Recent Changes
13 Codes in Apple's Passwords App
14 Google Prompts: Tap Yes to Sign In

Part 3 — Passkeys

15 Passkeys on iPhone, iPad and Mac
16 Passkeys on Android and in Google Password Manager
17 Passkeys with Samsung Pass
18 Passkeys on a Windows Computer
19 Make a Passkey for Your Google Account
20 Make a Passkey for Your Microsoft Account
21 Make a Passkey for Amazon
22 Make a Passkey for PayPal
23 Signing In on a Computer with Your Phone's Passkey
24 Your Apple Account's Two-Factor Authentication
25 Security Keys: The Little Key on Your Keychain

Part 4 — Spare Keys, New Phones & Lost Phones

26 Backup Codes: Your Spare Key
27 Moving to a New Phone: The Checklist

28 New Phone: Moving Google Authenticator
29 New Phone: Restoring Microsoft Authenticator
30 Lost, Broken or Stolen Phone
31 When Codes Don't Work

Part 5 — Scams, Family & Getting Help

32 Never Read a Code to Anyone
33 Surprise Sign-In Prompts (Push Bombing)
34 Fake Passkey Emails and Look-Alike Apps
35 Helping a Parent Set This Up
36 When to Call Bill
37 Your Authenticator & Passkey Cheat-Sheet

PART 1

The Big Picture

What the "second lock" on your accounts is, the different kinds, what a passkey really is, and a calm one-hour plan to get it all set up.

CHAPTER 1

A Note from Bill

Hello, and welcome. If you've ever been asked to "enter the six-digit code," told to "approve this sign-in on your phone," or invited to "create a passkey" and wondered what on earth that means, this guide is for you. These are all ways of putting a second lock on your accounts, so that a stolen password alone isn't enough for a stranger to get in.

I'm Bill. For more than 30 years I've helped people make sense of their technology, and I serve folks right here in Portage County, Ohio. I wrote this guide the way I'd explain it at your kitchen table: slowly, in plain English, one step at a time. Any word you might not know, I'll stop and explain.

Who this guide is for

- Anyone who has been asked to turn on two-step verification and isn't sure which choice to pick.
- Anyone using **Google Authenticator** or **Microsoft Authenticator** who wants to be sure the codes won't vanish with an old phone.
- Anyone curious about **passkeys**: the new way to sign in with your face, fingerprint or phone PIN instead of a password.
- Grown children and caregivers helping a parent, with that parent's blessing.

WHAT THIS DOES FOR YOU

What this guide does for you

By the end you'll understand the different kinds of second lock, set up the ones that suit you, make passkeys for the big accounts (Google, Microsoft, Amazon, PayPal), keep a spare way in with backup codes, move everything safely to a new phone, and spot the scams that try to trick you out of a code.

An honest promise about this topic

In most of my guides I tell you that you can't break anything by exploring. Here I'll be a little more careful. Looking around these settings is perfectly safe. But **turning on a second lock without a spare way in** is the one real mistake you can make, because if you then lose your phone you can lock *yourself* out. So every time we add a lock in this guide, we'll also set up a spare key. Follow that habit and you'll be safer and never stranded.

This guide sits alongside two others. *Passwords & Password Managers* covers making and storing strong passwords, and *Securing Your Accounts* walks through a full security tune-up. This one focuses on the codes, prompts and passkeys.

You're never stuck alone

If anything in this guide feels like too much, call or text me at **(330) 200-8042**. We'll sort it out together, with no judgment.

— Bill

CHAPTER 2

What Two-Step Verification Is

Think about your front door. A password is like a key. If someone copies your key, they can walk right in. **Two-step verification** adds a second lock that needs something only you have, usually your phone. Now a copied key isn't enough on its own.

The many names for the same idea

Different companies use different names, and they all mean roughly the same thing. You'll see **two-step verification** (Google), **two-factor authentication** or **2FA** (Apple and many banks), and **multi-factor authentication** or **MFA** (Microsoft and workplaces). In this guide I'll mostly say "two-step" or "the second lock."

How it feels day to day

1. You type your email and password, as usual.
2. The website asks for one more thing: a code from your phone, a tap on a prompt, or your fingerprint.
3. You give it, and you're in.
4. On a phone or computer you use every day, many sites remember you, so you won't be asked every time. You'll mostly see the second step on a new device or after a long while.

WHAT THIS DOES FOR YOU

Why it's worth the trouble

Passwords leak. Big companies get breached, and fake login pages trick careful people. With a second lock, a crook who has your password still hits a wall, because they don't have your phone.

GOOD TO KNOW

It isn't about whether you're careful

You can do everything right and still have a password show up in someone else's data breach. The second lock protects you from mistakes made by the companies, not just your own.

CHAPTER 3

Text Codes, Apps, Prompts, Passkeys and Keys

There are five common kinds of second lock. They all work. Some are simply harder for crooks to get around than others. Here they are, from the most familiar to the strongest.

Kind	What it is
Text or phone-call code	A six-digit code is texted to you or read by an automated call. Familiar and easy, but the weakest choice, because crooks can sometimes steal a phone number or trick you into reading the code to them.
Authenticator app code	An app on your phone (Google Authenticator, Microsoft Authenticator or Apple's Passwords app) shows a fresh six-digit code every 30 seconds. Works even with no signal. See Chapter 6, *How Authenticator Apps Work*.
Sign-in prompt	Your phone pops up "Are you trying to sign in?" and you tap **Yes** or match a number. Google calls these Google prompts; Microsoft uses its Authenticator app. See Chapter 14, *Google Prompts: Tap Yes to Sign In* and Chapter 11, *Approving Sign-Ins with Microsoft Authenticator*.
Passkey	You sign in with the same face, fingerprint or PIN you use to unlock your phone. No code to type and nothing a crook can trick out of you. See Chapter 4, *What a Passkey Really Is*.
Security key	A small physical key that plugs into a computer or taps against a phone. The strongest choice, mostly for people at higher risk. See Chapter 25, *Security Keys: The Little Key on Your Keychain*.

Which should you choose?

Google itself says codes by text or call "can be vulnerable to phone number-based hacks," and recommends passkeys first, then prompts. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) calls the passkey-style kind (FIDO) "phishing-resistant," meaning a fake website can't trick it. My plain-English advice is below.

1. Where a site offers **passkeys**, make one. They're the easiest and the safest.
2. Where it doesn't, use an **authenticator app** or **sign-in prompts**.
3. Keep a **text code** only as a backup, if the site allows it, and only if you can't use the others.
4. Whatever you pick, set up a **spare way in**: backup codes, a second phone number or email, or a second passkey. See Chapter 26, *Backup Codes: Your Spare Key*.

TIP

A text code is still far better than nothing

If text codes are the only thing you're comfortable with, use them. A second lock you actually use beats a better one you never set up.

CHAPTER 4

What a Passkey Really Is

A **passkey** is a new way to sign in that replaces your password. Instead of typing something, you unlock the sign-in the same way you unlock your phone: with your face, your fingerprint, or your phone's PIN or passcode. That's it. No password to remember, and no code to type.

What's going on behind the scenes

When you make a passkey, your phone or computer creates a matched pair of digital keys. One stays secret on your device (and in your Apple, Google or Samsung account if it syncs). The other is given to the website. When you sign in, the two keys check each other. The secret half never leaves your device, so there's nothing for a fake website to steal, and nothing for you to read out to a scammer.

Why passkeys are spreading so fast

- **They can't be phished.** A passkey only works on the real website it was made for. A look-alike site simply gets nothing.
- **Nothing to remember.** Your face or fingerprint does the work.
- **They're quick.** One glance or one touch.
- **The big companies are pushing them.** Since May 2025, Microsoft makes new personal accounts passwordless by default and offers passkeys first. Google says that once you create a passkey, it will offer it first when you sign in, though you can still use your password.

Where passkeys are kept

Device	Where your passkey lives
iPhone, iPad, Mac	In Apple's **Passwords** app, synced by iCloud Keychain to your other Apple devices. See Chapter 15, *Passkeys on iPhone, iPad and Mac*.
Android phones	In **Google Password Manager**, synced to your Google Account. See Chapter 16, *Passkeys on Android and in Google Password Manager*.
Samsung Galaxy	In **Samsung Pass** or Google Password Manager; you choose. See Chapter 17, *Passkeys with Samsung Pass*.
Windows computer	In **Windows Hello** on that computer, or in Google Password Manager if you use Chrome. See Chapter 18, *Passkeys on a Windows Computer*.
Security key	On the key itself. See Chapter 25, *Security Keys: The Little Key on Your Keychain*.

GOOD TO KNOW

"Passkey" is not "passcode"

Your phone's **passcode** (or PIN) is the number you type to unlock it. A **passkey** is the new sign-in for a website, and it uses that passcode, your face or your fingerprint to prove it's you. Different words, related idea.

HEADS UP

Make passkeys only on your own devices

Google's advice is to create passkeys only on phones and computers you personally own and use. Don't make one on a library computer or a friend's tablet, because anyone who can unlock that device could use it.

CHAPTER 5

Your One-Hour Safety Plan

You don't need to do everything in this guide. Here's the order I'd suggest, starting with the accounts that matter most. Do one a day if you like. There's no rush.

Start with your email account

Your email is the master key to everything else. If a crook gets into your email, they can use "forgot password" links to get into your bank, shopping and social accounts. So lock your email first.

1. **Your email account** (Gmail, Outlook.com, Yahoo, AOL or your internet provider's email). Turn on two-step, and make a passkey if offered. See Chapter 19, *Make a Passkey for Your Google Account* or Chapter 20, *Make a Passkey for Your Microsoft Account*.
2. **Your phone's main account**: your Apple Account on an iPhone, or your Google Account on Android. See Chapter 24, *Your Apple Account's Two-Factor Authentication*.
3. **Money accounts**: your bank, PayPal and any investment accounts. See Chapter 22, *Make a Passkey for PayPal*.
4. **Shopping**: Amazon and any store with your card saved. See Chapter 21, *Make a Passkey for Amazon*.
5. **Social media**: Facebook and similar, because crooks use hacked accounts to scam your friends.

For each account, the same three steps

1. Turn on the second lock (passkey, app or prompt).
2. Set up a spare way in: save the backup codes, or add a second phone number or email.
3. Write down where you put the spare key, in the "Keep this handy" table in Chapter 37, *Your Authenticator & Passkey Cheat-Sheet*.

> **TIP**
>
> **Use the official site or app, typed in by you**
>
> Always start from the company's own app or a web address you type yourself, such as **myaccount.google.com** or **account.microsoft.com**. Never from a link in an email or text.

FROM BILL

This is what my Digital Safety Check-Up covers

If you'd like a hand, my **Digital Safety Check-Up** walks through exactly this list with you. See Chapter 36, *When to Call Bill* for how to reach me.

PART 2

Authenticator Apps & Sign-In Prompts

Google Authenticator, Microsoft Authenticator, codes in Apple's Passwords app, and the tap-to-approve prompts from Google and Microsoft.

CHAPTER 6

How Authenticator Apps Work

An **authenticator app** is a free app that shows a six-digit code for each account you add. The code changes every 30 seconds or so. When a website asks for your code, you open the app, read the current code for that site, and type it in.

Why they're better than text codes

- **No signal needed.** The codes are worked out on your phone using the time of day, so they work in a basement, on a plane or out in the country with no bars. Google's help pages say so plainly.
- **Nobody can redirect them.** A crook who hijacks your phone number still can't get your app codes.
- **One app, many accounts.** You can keep codes for Google, Facebook, your bank and more in the same app.

The main choices

App	In a nutshell
Google Authenticator	Free from Google for iPhone and Android. Can back up your codes to your Google Account. See Chapter 7, *Google Authenticator: Getting Started*.
Microsoft Authenticator	Free from Microsoft for iPhone and Android. Does codes and also tap-to-approve prompts for Microsoft accounts. See Chapter 10, *Microsoft Authenticator: Getting Started*.
Apple Passwords app	Built into iPhone, iPad and Mac. Can store a code right alongside the password for that site. See Chapter 13, *Codes in Apple's Passwords App*.

TIP

Pick one and stick with it

Any of these works with nearly every website that says "use an authenticator app." The codes follow the same standard. Keeping all your codes in one app makes it easier to find them and to move them to a new phone later.

HEADS UP

The one big risk: losing the phone

If the codes live only on one phone and that phone is lost, the codes go with it. That's why each app section below shows you how to back them up, and why Chapter 26, *Backup Codes: Your Spare Key* matters so much.

CHAPTER 7

Google Authenticator: Getting Started

Google Authenticator is a simple, free code app from Google. You don't need a Gmail account to use it, but if you have one, signing in lets the app keep a backup copy of your codes.

Install it

1. On an iPhone, open the **App Store**. On Android, open the **Play Store**.
2. Search for **Google Authenticator**. Check that the maker is listed as **Google LLC**.
3. Tap **Get** or **Install**.
4. Open the app and tap **Get started**.
5. When it offers to sign in with your Google Account, I recommend you do. That turns on the backup described in Chapter 9, *Google Authenticator Backup: Sync with Your Google Account*.

SCAM ALERT

Watch out for look-alike apps

App stores sometimes carry copycat "authenticator" apps that charge a subscription. The real Google Authenticator is free. Check the maker's name before you install. See Chapter 34, *Fake Passkey Emails and Look-Alike Apps*.

Using Google Authenticator to sign in to Google itself

If you want codes for your Google Account, Google's steps are: go to your Google Account's 2-Step Verification settings, tap **Set up authenticator**, and follow the on-screen steps. Google also advises keeping a second method turned on so you can't lock yourself out.

GOOD TO KNOW

For your Google Account, prompts may be simpler

Many people find Google prompts (a tap on "Yes, it's me") easier than codes for their Google Account itself. Use Authenticator for the *other* websites that ask for an app. See Chapter 14, *Google Prompts: Tap Yes to Sign In*.

CHAPTER 8

Adding a Website to Your Authenticator App

Adding an account to an authenticator app usually means pointing your phone's camera at a square barcode (a **QR code**) that the website shows you. It sounds technical, and it's actually one of the easiest steps in this guide.

The usual steps

1. On your computer, sign in to the website you want to protect and find its security settings. Look for words like **Two-step verification**, **2FA**, **Security** or **Login & security**.
2. Choose **Authenticator app**. The website shows a QR code.
3. On your phone, open your authenticator app and tap the **plus sign (+)**.
4. Choose **Scan a QR code** and point the camera at the code on the computer screen.
5. The new account appears in the app with a six-digit code.
6. Type that code into the website to prove it worked.
7. If the website then offers **backup codes**, save them now. See Chapter 26, *Backup Codes: Your Spare Key*.

TIP

Setting up on the phone itself

If you're doing this on the same phone and can't scan your own screen, look for a link that says **Can't scan it?** or **Enter a setup key**. The website gives you a long string of letters to copy into the app instead.

STAY SAFE

Treat that QR code like a house key

Anyone who scans the same QR code gets your codes too. Never photograph it, email it, or show it to anyone, and never scan a QR code someone sends you claiming to be "security setup."

Give each account a clear name

Most apps let you rename an entry. If you have two accounts with similar names, rename them so you can tell them apart at a glance, such as "Gmail (mine)" and "Gmail (Mom's)."

CHAPTER 9

Google Authenticator Backup: Sync with Your Google Account

The best thing that's happened to Google Authenticator is **cloud sync**. When you're signed in to the app with your Google Account, your codes are backed up to that account. On a new phone, you sign in and your codes come back.

Check that sync is on

1. Open **Google Authenticator**.
2. Look at the top right. If you see your Google profile picture or initial, you're signed in and syncing.
3. If you see a cloud with a line through it or a sign-in button, tap it and sign in with your Google Account.

GOOD TO KNOW

You need a reasonably recent version

Google says sync needs version 6.0 or later of the app on Android, or version 4.0 or later on iPhone. If the app is very old, update it from the App Store or Play Store.

What sync means for a new phone

When you sign in to your Google Account inside Google Authenticator on a new phone, your codes are copied to it automatically. Without sync, you'd have to move them by hand with the transfer tool, or set up each website again. See Chapter 28, *New Phone: Moving Google Authenticator*.

HEADS UP

Keep your Google Account itself safe

With sync on, your Google Account holds the key to all your codes. That's one more reason to give your Google Account its own strong protection (a passkey or prompts) and backup codes. See Chapter 19, *Make a Passkey for Your Google Account*.

CHAPTER 10

Microsoft Authenticator: Getting Started

Microsoft Authenticator is Microsoft's free app for iPhone and Android. It does two jobs: it shows six-digit codes for any website (like Google Authenticator), and it lets you approve sign-ins to your **Microsoft account** (Outlook.com, Hotmail, Xbox, Microsoft 365) with a tap instead of a code.

Install it and add your Microsoft account

1. Install **Microsoft Authenticator** from the App Store or Play Store. Check the maker is **Microsoft Corporation**.
2. Open the app. Tap **Add account** (or the **plus sign**).
3. Choose **Personal account** for your own Outlook.com, Hotmail or Xbox account.
4. Sign in with your Microsoft account and follow the prompts.
5. For any other website, choose **Other account** and scan its QR code as in Chapter 8, *Adding a Website to Your Authenticator App*.

App Lock

Microsoft Authenticator has **App Lock**, which asks for your phone's PIN, face or fingerprint every time you open the app and before you approve a sign-in. Microsoft turns it on by default once your phone has a PIN or fingerprint set up. Leave it on: it means someone who picks up your unlocked phone still can't approve a sign-in. You'll find it in the app's **Settings**.

GOOD TO KNOW

Work and school accounts are different

If an employer or school asked you to install Authenticator, they control its settings. Follow their instructions for that account. This guide is about your personal accounts.

TIP

Turn on backup now

Before you add many accounts, turn on the app's backup so you can restore it on a new phone. See Chapter 29, *New Phone: Restoring Microsoft Authenticator*.

CHAPTER 11

Approving Sign-Ins with Microsoft Authenticator

Once your Microsoft account is in the app, signing in on a computer can be as simple as tapping your phone. This is called a **sign-in prompt** or **push notification**.

What it looks like

1. On the computer, type your Microsoft account email and choose to sign in with a notification if asked.
2. The computer shows a two-digit number.
3. Your phone shows a notification from Authenticator. Tap it.
4. Unlock the app with your face, fingerprint or PIN if asked.
5. Type the number you see on the computer screen, and tap **Yes** or **Approve**.

Why you have to type a number

This is called **number matching**. It proves you're looking at the very computer that's asking. CISA recommends it because it stops crooks from flooding your phone with prompts and hoping you tap Yes by accident. More on that in Chapter 33, *Surprise Sign-In Prompts (Push Bombing)*.

SCAM ALERT

If you didn't just try to sign in, tap Deny

A prompt you weren't expecting means someone else has your password and is trying to get in. Tap **Deny** or **No, it's not me**, then change your password from a device you trust.

TIP

No number box showing?

Microsoft says the box for typing the number may not appear if the app is locked. Open Authenticator, unlock it, and look again.

CHAPTER 12

Microsoft Authenticator's Recent Changes

Microsoft has changed Authenticator and Microsoft accounts quite a bit since 2025. If something you used to rely on disappeared, here's what happened.

Saved passwords moved to Microsoft Edge

Microsoft Authenticator used to save and fill in passwords. Microsoft removed that in 2025. Starting in June 2025 you could no longer save new passwords in it, autofill stopped in July, and by August saved passwords were no longer shown in Authenticator. The passwords were **not deleted**: they stay in your Microsoft account and are available in the **Microsoft Edge** browser. To keep filling them in on your phone, Microsoft's advice was to install Edge and make it your phone's autofill provider.

> **TIP**
>
> **Or move them somewhere else**
>
> You don't have to use Edge. You can use Apple's Passwords app, Google Password Manager or another password manager. Our guide *Passwords & Password Managers* walks through choosing one.

New Microsoft accounts don't need a password

Since May 1, 2025, new personal Microsoft accounts are passwordless by default. You sign in with a passkey, an Authenticator prompt or a code instead. Existing accounts keep their password unless you choose to remove it.

Text-message codes are being phased out

Microsoft has announced it will stop sending text-message (SMS) codes for personal Microsoft accounts, steering people to passkeys, the Authenticator app and a verified backup email instead. Reports put the start of this in 2026. If you've always signed in to Outlook.com or Hotmail with a texted code, set up a passkey and add a backup email address now, so you aren't caught out. See Chapter 20, *Make a Passkey for Your Microsoft Account*.

HEADS UP

Emails about this change can be faked

Microsoft did email customers about passkeys and the end of text codes. Crooks copy emails like that. Don't click the links: open **account.microsoft.com** yourself. See Chapter 34, *Fake Passkey Emails and Look-Alike Apps*.

CHAPTER 13

Codes in Apple's Passwords App

If you have an iPhone, iPad or Mac, you may not need a separate authenticator app at all. Apple's **Passwords** app can store the six-digit code for a website right alongside that site's password, and fill it in for you when you sign in.

Add a code for a website (iPhone)

1. On the website's security page, choose to set up an **authenticator app**. Keep the QR code or setup key on screen.
2. Open the **Passwords** app on your iPhone and tap **All**.
3. Tap the website's entry, then tap **Edit**.
4. Tap **Set Up Code** and enter the setup key, or scan the QR code if offered.
5. If the QR code is on your iPhone's screen, you can touch and hold it and choose **Add Verification in Passwords** instead.
6. Tap **Done**. Type the code shown into the website to finish.

Using the code

When the website asks for the code, it usually appears as a suggestion above the keyboard. Tap it. If it doesn't, open Passwords, find the account, and copy the code.

GOOD TO KNOW

It travels with your Apple Account

Passwords and passkeys in the Passwords app sync to your other Apple devices that are signed in to the same Apple Account with iCloud Keychain turned on. That makes a new iPhone much easier. See Chapter 27, *Moving to a New Phone: The Checklist*.

HEADS UP

Don't keep the only copy in one place

Some people prefer codes kept apart from passwords, so a single slip can't expose both. That's a fair choice. Either way, save the website's backup codes too.

CHAPTER 14

Google Prompts: Tap Yes to Sign In

For your Google Account, the simplest second lock is usually a **Google prompt**. When you sign in on a new device, your phone shows "Trying to sign in?" and you tap **Yes, it's me**.

Who can use them

- Android phones signed in to your Google Account.
- iPhones with the **Gmail**, **Google**, **Google Photos** or **YouTube** app signed in to that account.

Why Google recommends them

Google says prompts are quicker than typing a code and also help protect against SIM swaps and other phone-number tricks. If you don't use a passkey, Google recommends prompts as your second step.

Using a prompt

1. Sign in on the new device with your email and password.
2. Look at your phone. A prompt appears showing the device and roughly where it is.
3. If it's you, tap **Yes, it's me**. Sometimes Google asks you to tap a matching number too.
4. If it's not you, tap **No, it's not me**. Google will help you secure the account.

SCAM ALERT

Never tap Yes to make a prompt go away

A prompt you didn't ask for means someone has your password. Tapping Yes lets them in. Tap No, then change your password. See Chapter 33, *Surprise Sign-In Prompts (Push Bombing)*.

PART 3

Passkeys

Where your passkeys live on iPhone, Android, Samsung and Windows, how to make them for Google, Microsoft, Amazon and PayPal, and the extra protection on your Apple Account.

CHAPTER 15

Passkeys on iPhone, iPad and Mac

On Apple devices, passkeys are saved in the **Passwords** app, the same place as your saved passwords. With iCloud Keychain turned on, a passkey you make on your iPhone also appears on your iPad and Mac signed in to the same Apple Account.

Making a passkey on an iPhone

1. Sign in to the website or app as usual.
2. If the site supports passkeys, it will offer one, either right after you sign in or in its account or security settings. Look for **Create a passkey** or **Add a passkey**.
3. Your iPhone asks whether to save a passkey. Tap **Continue**.
4. Look at your iPhone (Face ID) or touch the sensor (Touch ID) to confirm. That's it.

Signing in with it

Next time, tap the email or username box on the site. Your iPhone suggests the passkey. Tap it, glance at the phone or touch the sensor, and you're in. If you don't see a passkey option, that site doesn't support passkeys yet, and you sign in the old way.

Seeing your passkeys

1. Open the **Passwords** app.
2. Tap **Passkeys** to see every site you've made one for.
3. Tap one to see its details. A site can hold both a passkey and a password in the same entry.

GOOD TO KNOW

Is iCloud Keychain on?

Syncing needs iCloud Keychain. In **Settings**, tap your name, then **iCloud**, and look for **Passwords** (on some versions, **Passwords and Keychain**). Make sure syncing is on. Without it, a passkey stays on that one device.

TIP

Delete one if you change your mind

Deleting a passkey from the Passwords app doesn't always remove it from the website, and vice versa. If you stop using one, remove it in both places.

CHAPTER 16

Passkeys on Android and in Google Password Manager

On Android phones, passkeys are normally saved to **Google Password Manager**, which is part of your Google Account. They're end-to-end encrypted, which means even Google can't read them, and they sync to your other devices signed in to the same Google Account.

Making a passkey on Android

1. Sign in to the website or app as usual.
2. When it offers to **create a passkey**, tap to continue.
3. If your phone asks where to save it, choose **Google Password Manager** (or Samsung Pass on a Galaxy; see Chapter 17, *Passkeys with Samsung Pass*).
4. Unlock with your fingerprint, face, PIN or pattern to confirm.

Your passkeys on a new device

Google encrypts each passkey on your device before syncing it. On a new device, you prove it's you by signing in to your Google Account and entering either your old Android phone's **screen lock** (PIN, pattern or password) or your **Google Password Manager PIN**. So remember your old phone's unlock code until the move is done.

Using your Google passkeys on an iPhone or computer

- **On a computer:** in Chrome, signed in to your Google Account, your Google Password Manager passkeys are available. Chrome may ask you to create a Google Password Manager PIN the first time.
- **On an iPhone or iPad:** Google says this needs iOS or iPadOS 17 or later, and you set Chrome as an autofill provider in your iPhone's settings.
- Google notes you can't create or reset the Password Manager PIN on an Android phone itself; you do that from Chrome on a computer, iPhone, iPad or Chromebook.

TIP

Write the PIN down

Write your Google Password Manager PIN in the "Keep this handy" table in Chapter 37, *Your Authenticator & Passkey Cheat-Sheet*, and keep it somewhere safe at home.

CHAPTER 17

Passkeys with Samsung Pass

Samsung Galaxy phones have their own password and passkey keeper called **Samsung Pass**, tied to your **Samsung Account**. Samsung says passkeys are supported on Galaxy phones with **One UI 6 or later**. Samsung Pass now lives inside the **Samsung Wallet** app on many phones.

Choosing Samsung Pass or Google

When a Galaxy phone offers to save a passkey, it may ask whether to use Samsung Pass or Google Password Manager. Either is safe. Here's how I'd decide:

Choice	Good for
Google Password Manager	Best if you might ever switch to a non-Samsung Android phone, or want your passkeys in Chrome on your computer.
Samsung Pass	Fine if you're sure you'll stay with Galaxy phones. Your passkeys follow your Samsung Account.

TIP

Pick one and stay with it

Splitting passkeys between the two makes them harder to find. Choose one and make it your habit.

A passkey for your Samsung Account itself

1. Open **Settings** and tap your name at the top.
2. Under **Security and privacy**, tap **Set up a passkey** (the wording may vary a little).
3. Tap **Create passkey** and confirm with your fingerprint or screen lock.

CHAPTER 18

Passkeys on a Windows Computer

On a Windows computer, passkeys can be saved two ways. Knowing which one you used tells you whether that passkey will follow you to another device.

Saved in	What that means
Windows Hello	Saved on **that computer only**. You confirm with the computer's PIN, face camera or fingerprint reader. Google's help pages note these aren't synced or backed up.
Google Password Manager in Chrome	Saved to your Google Account and available wherever you're signed in to Chrome or Android with the same account. See Chapter 16, *Passkeys on Android and in Google Password Manager*.

Making one

1. Sign in to the website in your browser.
2. Choose to create a passkey in the site's security settings, or when it offers.
3. A Windows or Chrome box asks where to save it. Choose the one you want.
4. Confirm with your computer's PIN, face or fingerprint.

HEADS UP

Replacing the computer?

A Windows Hello passkey stays behind with the old computer. Before you retire it, make sure you have another way in to each site: a passkey on your phone, or your password and second step.

TIP

Your phone works too

You can sign in on a computer using a passkey stored on your phone, by scanning a QR code. See Chapter 23, *Signing In on a Computer with Your Phone's Passkey*.

If you're moving to a new Windows computer, our guide *Moving to a New Windows PC* covers the rest of the move.

CHAPTER 19

Make a Passkey for Your Google Account

Your Google Account covers Gmail, YouTube, Google Photos and, on Android, your whole phone. It's one of the best places to start with passkeys.

The steps

1. On the phone or computer you'll sign in with, go to **myaccount.google.com/signinoptions/passkeys**. (Or open your Google Account, tap **Security**, and find **Passkeys and security keys**.)
2. Sign in if asked.
3. Tap **Create a passkey**, then **Create a passkey** again.
4. Unlock your device with your face, fingerprint or PIN when asked.
5. You'll see the new passkey in the list.

What you need

- A phone with Android 9 or iOS 16 or later, or
- A computer with Windows 10, macOS Ventura or ChromeOS 109 or later, and a recent browser (Chrome, Safari, Edge or Firefox), or
- A FIDO2 security key (choose **Use another device** when creating). See Chapter 25, *Security Keys: The Little Key on Your Keychain*.

GOOD TO KNOW

Your password still works

Google says making a passkey puts you on "passkey-first" sign-in, but you can still choose your password if you need to. Keep 2-Step Verification and backup codes in place as your spare key.

HEADS UP

Work or school Google accounts

If your Gmail comes from an employer or school, they may not allow signing in with just a passkey. Ask them.

CHAPTER 20

Make a Passkey for Your Microsoft Account

Your Microsoft account is what you use for Outlook.com or Hotmail email, Windows, Xbox, OneDrive and Microsoft 365. With Microsoft phasing out text-message codes (see Chapter 12, *Microsoft Authenticator's Recent Changes*), a passkey is now the easiest way to keep getting in.

The steps

1. Go to **account.microsoft.com** and sign in. Choose **Security**.
2. Look for the option to **add a new way to sign in or verify**. (Microsoft also lists the direct address **account.live.com/proofs/manage**.)
3. Choose **Face, Fingerprint, PIN, or Security key**.
4. Follow your device's prompts. It may offer to save the passkey on this computer (Windows Hello), on your phone by scanning a QR code, in a password manager, or on a security key.
5. Give the passkey a name you'll recognize, such as "My iPhone."

TIP

The easy way: "Sign in faster"

When you sign in, Microsoft may offer **Sign in faster** with a passkey. Choosing **Next** walks you through making one.

Also add a backup email

While you're on the Security page, make sure a second email address you can get into is listed as a way to verify. With text codes going away, that backup email is your spare key if a passkey device is lost.

GOOD TO KNOW

Work or school Microsoft accounts

Those are managed at **mysignins.microsoft.com**, and only if your organization allows it.

CHAPTER 21

Make a Passkey for Amazon

Amazon supports passkeys, so you can sign in to shop with your face or fingerprint instead of a password. Because Amazon holds your card and address, it's well worth doing.

The steps

1. Open Amazon (the app or amazon.com) and go to **Your Account**.
2. Choose **Login & security**. You may be asked to sign in again.
3. Next to **Passkey**, tap **Set up**.
4. Tap **Set up** again and follow your phone's or computer's prompts to confirm with your face, fingerprint or PIN.

Good to know about Amazon passkeys

- The passkey is saved to your passkey keeper, such as your Apple or Google account.
- Amazon allows **one passkey per passkey keeper**. So you can have one in Apple Passwords and one in Google Password Manager, but not two in the same one.
- Amazon lists the minimums as iOS 16, macOS Big Sur, Android 9 or Windows 11, with an up-to-date browser.
- A passkey made on amazon.com doesn't carry over to other Amazon country sites, such as amazon.co.uk.

SCAM ALERT

Amazon will never call you about your passkey

Calls, texts or emails saying "your Amazon passkey has been compromised" or asking you to read a code are scams. Hang up and check your account in the Amazon app yourself.

CHAPTER 22

Make a Passkey for PayPal

PayPal supports passkeys for personal accounts. Because PayPal moves real money, a passkey is a strong upgrade over a password and texted code.

The steps (on your phone)

1. On your phone, open **Safari** (iPhone) or **Chrome** (iPhone or Android) and go to **paypal.com**.
2. Log in the usual way with your email and password.
3. If your account is eligible, PayPal offers to create a passkey. Review the details and tap to continue.
4. Unlock your phone with your face, fingerprint or passcode to finish.

Things PayPal points out

- Passkeys are created on phones, through the Safari or Chrome browser, for eligible personal and Premier accounts.
- PayPal lists support on iOS 16, iPadOS 16, macOS Ventura and Android 9 or later. Its help page says passkeys aren't supported on Windows devices.
- To log in on a computer, choose **Other options** or **Passkey from a nearby device**, scan the QR code with your phone, and approve. See Chapter 23, *Signing In on a Computer with Your Phone's Passkey*.
- If you delete a passkey in PayPal, also remove it from your password manager, or your phone may keep offering it.

SCAM ALERT

PayPal codes are for you alone

Scammers posing as PayPal, or as a buyer on Marketplace, often ask for "the code PayPal just sent you." Never share it. Our *PayPal* guide covers these scams in more depth.

CHAPTER 23

Signing In on a Computer with Your Phone's Passkey

What if your passkey is on your phone, but you're signing in on a computer, or on a Windows PC when your passkeys are in Apple's Passwords app? You can use your phone as the key, with a QR code.

How it works

1. On the computer, start signing in to the website and choose the passkey option.
2. When asked where your passkey is, choose something like **Use a phone or tablet**, **Use another device** or **Passkey from a nearby device**. A QR code appears.
3. On your phone, open the **Camera** and point it at the QR code.
4. Tap the message that appears, then confirm with your face or fingerprint.
5. Keep the phone near the computer. Bluetooth is used to check the two are in the same room.
6. The computer signs you in.

WHAT THIS DOES FOR YOU

Why this is safe

Because the phone has to be physically near the computer, a crook across the world can't use this trick even with a convincing fake website.

SCAM ALERT

Never scan a passkey QR code someone sends you

Only scan a QR code that appears on a screen in front of you, after *you* started signing in. If a stranger emails, texts or shows you a QR code "to verify your account," don't scan it.

TIP

Bluetooth needs to be on

If the QR code step fails, check that Bluetooth is turned on on both the phone and the computer.

CHAPTER 24

Your Apple Account's Two-Factor Authentication

Your Apple Account (what Apple used to call an Apple ID) already uses two-factor authentication on most iPhones. When you sign in on a new device, Apple shows a six-digit code on one of your **trusted devices** or sends it to a **trusted phone number**.

Piece	What it does
Trusted device	An iPhone, iPad, Mac, Apple Watch or Apple Vision Pro already signed in with two-factor authentication. Codes pop up here.
Trusted phone number	A number that can receive the code by text or automated call. Apple advises having at least one.
Recovery key (optional)	A 28-character code you can create for extra control. Apple can't give it back if you lose it, and creating one turns off Apple's normal account recovery.
Security keys (optional)	Physical keys. Apple requires at least two, and allows up to six. See Chapter 25, *Security Keys: The Little Key on Your Keychain*.

The most important thing to check

Apple warns that if your iPhone is your **only** trusted device and holds your **only** trusted phone number, losing it may leave you unable to get codes. Add a second trusted number, such as a spouse's cell or your home phone that can take an automated call.

1. Open **Settings** and tap your name.
2. Tap **Sign-In & Security**.
3. Next to **Trusted Phone Numbers**, tap **Edit**, then **Add a Trusted Phone Number**.
4. Enter the number, choose text or phone call, and confirm with the code that arrives.

HEADS UP

Think twice about a recovery key

A recovery key gives you more control, but if you lose it and your devices, Apple can't help you back in. For most people, two trusted phone numbers is the safer choice. If you do make one, store it with your important papers.

GOOD TO KNOW

If you're truly locked out

If you have no trusted device or number, Apple's account recovery can get you back in, but Apple says it may take several days or longer. Start it at **iforgot.apple.com**, which is free.

CHAPTER 25

Security Keys: The Little Key on Your Keychain

A **security key** is a small device, about the size of a house key, that plugs into a computer's USB port or taps against the back of a phone. It holds a passkey that never leaves it. It's the strongest second lock there is, and it's mostly for people at higher risk: those who've been targeted before, public figures, or anyone who wants the very best.

What to look for

- **FIDO2** or **FIDO Certified** on the package. Google, Microsoft and Apple all work with FIDO keys.
- A plug that fits your devices: USB-C for most new computers and phones, USB-A for older computers, and **NFC** if you want to tap it against a phone.
- Buy **two**: one to carry, one to keep at home. Apple requires at least two for your Apple Account.

HEADS UP

Security keys can't be backed up

Google notes that passkeys stored on a security key aren't backed up. If you lose or reset the key, those passkeys are gone. That's why you always register two keys, plus a backup method, on every account.

GOOD TO KNOW

They cost money

Unlike apps and passkeys on your phone, security keys are something you buy, from the maker or an electronics store. Prices vary by model; check current prices before buying, and buy only from the maker or a store you trust, not an unknown seller.

TIP

Most people don't need one

For most folks, passkeys on your phone plus backup codes are plenty. A security key is an option, not a requirement.

PART 4

Spare Keys, New Phones & Lost Phones

Backup codes, moving your codes and passkeys to a new phone, what to do when a phone is lost or broken, and what to try when a code just won't work.

CHAPTER 26

Backup Codes: Your Spare Key

Backup codes are a short list of one-time codes a website gives you for emergencies. If your phone is lost, broken or dead, you type one of these instead of the usual code. They're the spare key under the flowerpot, except much safer, because you keep them indoors.

Google's backup codes

1. Go to **myaccount.google.com** and choose **Security**.
2. Tap **2-Step Verification** and sign in if asked.
3. Find **Backup codes** and tap it.
4. Google shows a set of **10 codes**, each 8 digits long. Choose to **download** or **print** them.
5. Keep the printout with your important papers.

How they work

- Each code works **once**. After you use it, cross it off.
- You can get a fresh set of 10 whenever you like. Getting a new set cancels the old set.
- Many other sites (Facebook, Amazon, banks and more) offer backup codes too. Look for them right after you turn on two-step, and save them every time.

TIP

Where to keep them

Google suggests a secure place such as with your passport or other important documents. A fire-safe box or the folder where you keep your will is ideal. Write on the outside which account they're for.

SCAM ALERT

Backup codes are for you alone

No bank, tech company or government office will ever ask you to read a backup code to them. Anyone who does is trying to break into your account. See Chapter 32, *Never Read a Code to Anyone*.

HEADS UP

Not on the same phone

Don't store backup codes only on the phone they're meant to replace. If the phone is lost, so are the codes. Paper at home, or a password manager you can open from another device, is the right place.

CHAPTER 27

Moving to a New Phone: The Checklist

Getting a new phone is exciting, and it's also the moment people most often lock themselves out. The golden rule is simple: **don't wipe or trade in the old phone until the new one is working for every account.**

Before you start

1. Make sure your backup codes are printed and nearby. See Chapter 26, *Backup Codes: Your Spare Key*.
2. Know your old phone's passcode or PIN. Google Password Manager may ask for it to unlock your passkeys on the new phone.
3. Charge both phones and connect to your home Wi-Fi.

What moves by itself, and what doesn't

Kind	On a new phone
Passkeys in Apple Passwords	Move with your Apple Account and iCloud Keychain to a new iPhone. See Chapter 15, *Passkeys on iPhone, iPad and Mac*.
Passkeys in Google Password Manager	Move with your Google Account. You may be asked for your old screen lock or Password Manager PIN. See Chapter 16, *Passkeys on Android and in Google Password Manager*.
Google Authenticator codes	Move automatically **if** the app was signed in to your Google Account. Otherwise, use the transfer tool. See Chapter 28, *New Phone: Moving Google Authenticator*.
Microsoft Authenticator codes	Restore from the app's backup, **if** you turned it on, and only iPhone to iPhone or Android to Android. See Chapter 29, *New Phone: Restoring Microsoft Authenticator*.
Text-message codes	Follow your phone number, as long as you keep the same number.
Windows Hello passkeys	Stay on that computer. Not affected by a new phone.

After the move

1. On the new phone, open each authenticator app and check your accounts are there.
2. Test-sign in to your most important accounts (email, bank) using the new phone.
3. Only when everything works, erase the old phone.

HEADS UP

Switching between iPhone and Android

Apple and Google keep their passkeys in separate systems. Google notes that a passkey in Google Password Manager isn't automatically available in Apple's system, and vice versa. If you switch sides, plan to make new passkeys on the new phone, using your password and second step to sign in the first time.

CHAPTER 28

New Phone: Moving Google Authenticator

If Google Authenticator was signed in to your Google Account, this is easy. If not, you'll use the app's **Transfer accounts** tool, which moves codes from the old phone to the new one by QR code.

The easy way: sign in

1. Install **Google Authenticator** on the new phone.
2. Open it and sign in with the same Google Account.
3. Your codes appear automatically.

The manual way: transfer by QR code

1. Install Google Authenticator on the new phone.
2. On the **old** phone, open Google Authenticator, tap the **menu** (three dots or lines), then **Transfer accounts**, then **Export accounts**.
3. Choose the accounts to move and tap **Next**. The old phone shows a QR code. If you move several accounts, it may show more than one.
4. On the **new** phone, tap **Scan QR code** (or **Transfer accounts**, then **Import accounts**) and scan each code from the old phone.
5. Check every account appears on the new phone.

HEADS UP

If the old phone is already gone

Without sync and without the old phone, the codes can't be recovered. You'll need to sign in to each site with a backup code or other method, remove the old authenticator, and set it up again on the new phone.

TIP

Turn on sync while you're there

Once the codes are on the new phone, sign the app in to your Google Account so next time is automatic. See Chapter 9, *Google Authenticator Backup: Sync with Your Google Account*.

CHAPTER 29

New Phone: Restoring Microsoft Authenticator

Microsoft Authenticator can back up your accounts, but only if you turned the backup on beforehand. Do that now, even if a new phone is a long way off.

Turn on backup (on the phone you have now)

Phone	Where the backup goes
iPhone	Authenticator backs up to **iCloud**. In the app, go to **Settings** and turn on **iCloud Backup**. Your iPhone also needs iCloud Keychain on, and Authenticator allowed to use iCloud.
Android	Authenticator backs up to a **personal Microsoft account** (an Outlook.com or Hotmail address). In the app, go to **Settings**, find **Backup**, and turn on **Cloud Backup**.

Restore on the new phone

1. Install **Microsoft Authenticator** on the new phone.
2. Open it, and **before adding any account**, tap **Restore from backup** or **Begin recovery**.
3. Sign in with the same iCloud (iPhone) or personal Microsoft account (Android) the backup used.
4. Your accounts come back. Some may show **Action required**: tap each one and sign in again.

What does and doesn't come back

- Six-digit codes for other websites usually restore fully.
- Accounts that used tap-to-approve sign-in restore only the account **name**. You sign in again to re-approve the phone.
- Work or school accounts need setting up again through your employer.
- Backups **don't cross over**: an iPhone backup can't be restored on Android, or the other way around.

HEADS UP

Microsoft can't restore it for you

If you didn't turn on backup, or can't get into the iCloud or Microsoft account that holds it, Microsoft support can't recover your codes. You'd sign in to each site another way and set it up again. That's why backup codes matter.

CHAPTER 30

Lost, Broken or Stolen Phone

Losing the phone that holds your codes and passkeys is upsetting, but it's very fixable if you've set up a spare key. Take a breath and go in this order.

First hour

1. **Try to find or lock the phone.** Use Find My (iPhone) or Find Hub (Android) from another device. Our guide *Lost or Stolen Phone* covers this step by step.
2. **Call your carrier** if the phone was stolen, to suspend the line. That stops anyone using your number for text codes.
3. **From a safe device** (a computer or tablet you trust), sign in to your email account using a backup code, a passkey on another device, or another method.
4. **Change your email password** and review the devices signed in to it. Remove the lost phone.

Over the next few days

1. Get a replacement phone and set it up. Passkeys and synced codes come back with your Apple or Google Account. See Chapter 27, *Moving to a New Phone: The Checklist*.
2. For each site whose codes lived only on the lost phone, sign in with a backup code, then remove the old authenticator and set it up again.
3. In your Google Account, Microsoft account and Apple Account, remove the lost phone from the list of devices and passkeys.
4. Print fresh backup codes for any site where you used one.

> **GOOD TO KNOW**
>
> **Apple Account: a trusted number can save the day**
>
> If you set up a second trusted phone number (see Chapter 24, *Your Apple Account's Two-Factor Authentication*), Apple can send your code there. If you have no trusted device or number, Apple's account recovery is free but can take several days.

SCAM ALERT

"Recovery experts" are a second scam

After a lost phone or lockout, people search online and find "account recovery services" that charge a fee or ask for your codes. Google, Microsoft, Apple and Amazon recovery is free through their own sites. Our guide *Hacked Account Recovery* lists the real pages.

CHAPTER 31

When Codes Don't Work

If a code keeps getting rejected, don't panic, and don't keep guessing too fast, because some sites lock you out after several wrong tries. Work through these one at a time.

Problem	What to try
"Wrong code" from an app	Wait for a fresh code and type it quickly, before the little timer runs out. Make sure you're reading the right account's code.
Codes always wrong	Your phone's clock may be off. Authenticator codes depend on the exact time. In your phone's date and time settings, turn on **Set Automatically** (iPhone) or **automatic date and time** (Android).
Text code never arrives	Check you have signal, wait a minute, and use **Resend** once. Check the phone number on file is still yours.
Prompt never arrives	Open the app (Gmail, Google or Authenticator) by hand. Check notifications are allowed and the phone is online. Choose **Try another way** on the sign-in screen.
Passkey not offered	The site may not support passkeys on that device, or the passkey is in a different keeper (Apple vs Google). Use **Try another way** or your phone's QR option. See Chapter 23, *Signing In on a Computer with Your Phone's Passkey*.
Code typed into the wrong site	If you typed a code into a page you're now unsure of, change that account's password from the official app straight away.

TIP

"Try another way" is your friend

Nearly every sign-in screen has a link called **Try another way**, **More options** or **Use a different method**. It lists all your second locks, including backup codes.

HEADS UP

Don't remove two-step to "fix" it

Turning off two-step to get past a hiccup leaves the account wide open. Fix the cause instead, or call for help.

If you've tried everything here and still can't get in, it's a good time to call. See Chapter 36, *When to Call Bill*.

PART 5

Scams, Family & Getting Help

The tricks crooks use to get around your second lock, how to help a parent set this up, when to call Bill, and a cheat-sheet to keep handy.

CHAPTER 32

Never Read a Code to Anyone

This is the single most important rule in this guide. A verification code is the second lock's key. **If you read it to someone, you've handed them the key.** Scammers know two-step works, so instead of breaking it, they try to talk you into giving them the code.

The FTC's rule

The Federal Trade Commission says it plainly: **anyone who asks you for your account verification code is a scammer.** Don't share a code with anyone who contacted you first, no matter who they say they are.

How the trick usually sounds

What they say	What's really happening
"Your bank's fraud department"	"We've stopped a suspicious charge. To confirm it's you, read me the code we just texted." The code is really letting them into your account.
"Amazon" or "Microsoft" support	"Your account is compromised. I'm sending a code to secure it." There is no such process.
A buyer on Marketplace or Craigslist	"I want to be sure you're real. I'll text you a code, read it back." The FTC warns this is used to set up a Google Voice number in your name.
A friend's hacked account	"Oops, I sent my code to your phone by mistake, can you send it to me?" It's the crook, using your friend's account to get into yours.

SCAM ALERT

The three-second test

Did *you* just try to sign in to something? If not, the code isn't for anyone. Don't read it, don't forward it, don't type it into a link someone sent you. Read the text itself: many say "Don't share this code with anyone. We'll never call to ask for it."

If you already gave a code away

1. Hang up or stop replying. Don't argue.
2. From the company's official app or website (typed in yourself), change that account's password.
3. Check the account's security page for new devices, new phone numbers or new email addresses you didn't add, and remove them.

4. If it's a bank or money account, call the number on the back of your card or on your statement.
5. Report it at **ReportFraud.ftc.gov**.

STAY SAFE

It isn't your fault

These callers are professionals who practice sounding official and urgent. Careful people get caught every day. What matters is acting quickly once you notice.

CHAPTER 33

Surprise Sign-In Prompts (Push Bombing)

Sometimes a crook who already has your password sends sign-in prompt after prompt to your phone, at all hours, hoping you'll tap **Approve** just to make them stop. Security people call this **MFA fatigue** or **push bombing**. CISA describes it as bombarding someone with push notifications until they approve.

What to do

1. **Tap Deny** (or **No, it's not me**) every time. Never Approve a prompt you didn't start.
2. Recognize what it means: **someone has your password**.
3. From a trusted device, **change that account's password** right away. The prompts stop once the old password no longer works.
4. Better still, make a passkey for that account so a password alone is useless. See Chapter 20, *Make a Passkey for Your Microsoft Account* or Chapter 19, *Make a Passkey for Your Google Account*.

SCAM ALERT

Watch for a "helpful" phone call

Push bombing is sometimes paired with a call: "This is Microsoft security. You'll get a prompt; please approve it so we can stop the attack." No real company does that. Hang up and tap Deny.

Why number matching helps

Microsoft Authenticator and some Google prompts ask you to type or tap a number shown on the computer screen. If you aren't at that computer, you can't know the number, so you can't approve by accident. CISA recommends number matching for exactly this reason. See Chapter 11, *Approving Sign-Ins with Microsoft Authenticator*.

TIP

Approved one by mistake?

Don't be embarrassed. Change the password right away, then open the account's security page and sign out of all other devices. If it's your email, check that no forwarding rules or new recovery details were added.

CHAPTER 34

Fake Passkey Emails and Look-Alike Apps

As passkeys and new sign-in rules make the news, crooks follow. Here are the newer tricks to watch for.

"Set up your passkey now" emails

Real companies do send emails encouraging passkeys, and Microsoft emailed customers about passkeys and the end of text codes. Fake versions copy the logos and add a deadline: "Set up by Friday or lose access." The link goes to a fake sign-in page.

SCAM ALERT

Never set up security from a link

Always go to the account yourself: type **myaccount.google.com**, **account.microsoft.com** or **amazon.com**, or open the official app. If the email was real, the same option will be waiting there.

Look-alike authenticator apps

- Check the maker before installing: **Google LLC** for Google Authenticator, **Microsoft Corporation** for Microsoft Authenticator.
- The real apps from Google and Microsoft are free. An "authenticator" asking for a weekly or monthly subscription is not one of them.
- Apple's Passwords app is already on your iPhone, iPad and Mac. You never need to download it.

Fake "your code" pages

A fake login page can ask for your password *and* your six-digit code, then use both within seconds. This is the main way crooks get past codes and prompts. It's also why passkeys are safer: a passkey simply won't work on a fake site.

TIP

A good sign you're on a fake page

If your password manager or phone doesn't offer to fill in your password or passkey on a page where it normally does, stop. It may not recognize the site because it isn't the real one.

CHAPTER 35

Helping a Parent Set This Up

If you're a son, daughter or caregiver, two-step and passkeys can make a parent much safer, as long as they're set up so your parent can actually use them, and with their blessing.

Good principles

- **Sit together and let them hold the phone.** They'll remember it better, and it stays their account.
- **Choose the simplest second lock they'll use.** For many people that's passkeys or tap-to-approve prompts rather than typing codes.
- **Add yourself as a backup, not a replacement.** For example, add your cell as a second trusted phone number on their Apple Account, if they agree.
- **Print the backup codes** and file them with their important papers, and note where in the table in Chapter 37, *Your Authenticator & Passkey Cheat-Sheet*.

If you live far away

Codes and prompts go to *their* phone, so you can't help sign in from your own. That's by design. Arrange a time to talk them through it by phone or video. Our guide *Helping a Parent from Afar* has more ideas.

STAY SAFE

Have "the code talk"

Agree on one simple family rule: **"We never read a code to anyone who calls. Not even me."** If a caller ever claims to be you and asks for a code, your parent will know it's a scam.

HEADS UP

Respect their independence

Don't make yourself the only person who can get into their accounts. If something happened to your phone, they'd be stuck. Their own phone, plus backup codes at home, is the right setup.

CHAPTER 36

When to Call Bill

Most of this guide you can do on your own, at your own pace. But some situations are worth a second pair of hands, especially when a mistake could lock you out.

Good reasons to call

- You'd like your important accounts set up with passkeys and two-step, and backup codes printed, all in one go.
- You're getting a new phone and want to be sure your authenticator codes and passkeys come with you.
- You've lost a phone and can't get into an account.
- You read a code to someone, or approved a prompt you shouldn't have, and want to lock things down.
- Microsoft or another company has stopped sending text codes and you're not sure what to set up instead.
- You're helping a parent and want everything set up the same way on their devices.

FROM BILL

My Digital Safety Check-Up

This guide pairs with my **Digital Safety Check-Up**. Together we go through your email, Apple or Google account, money and shopping accounts, turn on the right second lock for each, make passkeys where they help, and set up your spare keys so you're never stranded.

SCAM ALERT

I'll never ask for your codes

When I help, you hold the phone and type or approve things yourself. I'll never ask you to read me a code, and I'll never call out of the blue about your accounts.

How to reach me

Call or text **(330) 200-8042**, or book online at **billshometech.com/book**. Bill's Home Tech serves **Portage County, Ohio**, with 30+ years of professional experience. If you reach my assistant **Sophie** on the main line, she can answer simple questions and get you on my schedule. My help is **$49 remote · $99 in your home**. The guides themselves are free to read.

— Bill

CHAPTER 37

Your Authenticator & Passkey Cheat-Sheet

The most-used steps from this guide, in one place.

Where to go

I want to…	Do this
Google passkey	myaccount.google.com/signinoptions/passkeys, then **Create a passkey**. Chapter 19, *Make a Passkey for Your Google Account*
Google backup codes	myaccount.google.com > **Security** > **2-Step Verification** > **Backup codes**. Chapter 26, *Backup Codes: Your Spare Key*
Microsoft passkey	account.microsoft.com > **Security** > add a way to sign in > **Face, Fingerprint, PIN, or Security key**. Chapter 20, *Make a Passkey for Your Microsoft Account*
Amazon passkey	**Your Account** > **Login & security** > **Passkey** > **Set up**. Chapter 21, *Make a Passkey for Amazon*
PayPal passkey	Log in on your phone in Safari or Chrome and accept the passkey offer. Chapter 22, *Make a Passkey for PayPal*
Apple trusted number	**Settings** > your name > **Sign-In & Security**. Chapter 24, *Your Apple Account's Two-Factor Authentication*
See your Apple passkeys	**Passwords** app > **Passkeys**. Chapter 15, *Passkeys on iPhone, iPad and Mac*

New phone

App	What to do
Google Authenticator	Sign in to the app with your Google Account, or **Transfer accounts** > **Export accounts** on the old phone. Chapter 28, *New Phone: Moving Google Authenticator*
Microsoft Authenticator	Turn on backup first; on the new phone tap **Restore from backup** before adding accounts. Chapter 29, *New Phone: Restoring Microsoft Authenticator*
Old phone	Don't erase it until every account works on the new one. Chapter 27, *Moving to a New Phone: The Checklist*

Five safety rules

1. Never read a code to anyone, ever.
2. Tap Deny on any prompt you didn't start, then change that password.

3. Set up security only from the official app or an address you type yourself.
4. Every lock gets a spare key: backup codes, a second number or a second passkey.
5. Don't wipe an old phone until the new one works for every account.

Keep this handy

Item	My notes
Where my backup codes are kept	_____
My authenticator app	_____
Google Password Manager PIN hint	_____
Second trusted phone number (Apple)	_____
Backup email for Microsoft account	_____
Accounts with passkeys	_____
Bill's Home Tech	(330) 200-8042 · billshometech.com/book

FROM BILL

You've got this

A second lock and a spare key on your most important accounts puts you ahead of most crooks. Take it one account at a time, and call me at (330) 200-8042 if you'd like a hand.

— Bill