BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

Securing Your Accounts

Strong passwords, two-step sign-in, and staying a step ahead of the scammers — in plain English

A calm, practical guide to staying safe online

A few simple habits protect almost everything

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

Covers passwords, 2FA, passkeys & account recovery · facts current November 2026

What's Inside

This is your plain-English guide to keeping your online accounts safe — your email, your bank, your shopping and social accounts, and everything behind a password. Read it in any order and at your own pace. You don't need to be an expert, and you won't be asked to become one: the whole point of this book is that a **small handful of simple habits** protects almost everything. We'll go slowly, define every term, and focus on what truly matters. By the end you'll be a hard target for the scammers — and far more relaxed about living your life online.

Part 1 — Why This Matters & How to Think About It

1 A Note from Bill
2 What "Securing Your Accounts" Means
3 How Accounts Actually Get Broken Into
4 The Few Habits That Do Most of the Work

Part 2 — Strong Passwords & Password Managers

5 What Makes a Password Strong
6 The Reuse Trap
7 Password Managers Explained
8 Setting Up a Password Manager
9 Using a Password Manager Day to Day
10 Writing Passwords Down — the Safe Way

Part 3 — The Second Lock: Two-Step Verification

11 What Two-Step Verification Is
12 The Three Kinds of Second Step
13 Text-Message Codes
14 Authenticator Apps
15 Passkeys — the New Best Way
16 Turning It On, and Backup Codes

Part 4 — Recognizing the Tricks

17 Phishing: the Fake-Message Trick
18 Spotting a Phishing Email or Text
19 Fake Login Pages & Websites
20 Scam Phone Calls & "Tech Support"
21 Urgency, Fear & Too-Good-to-Be-True
22 Links & Attachments: Look Before You Click

Part 5 — Protecting Your Key Accounts

23 Your Email: the Master Key
24 Locking Down Your Email
25 Your Bank & Financial Accounts
26 Shopping & Everyday Accounts
27 Social Media Accounts
28 Your Phone, Its Lock & Device Accounts

Part 6 — If Something Goes Wrong

29 Signs Something May Be Wrong
30 What to Do If an Account Is Hacked
31 Recovering a Locked-Out Account
32 If Your Email Is Compromised
33 Identity Theft: the Basics
34 Keeping Calm & Acting Fast

Part 7 — Habits, Answers & When to Call Bill

35 Your Simple Security Routine
36 Questions People Ask Me All the Time
37 When to Call Bill
38 Your Account-Security Cheat-Sheet

PART 1

Why This Matters & How to Think About It

What "securing your accounts" really means, how accounts actually get broken into, and the reassuring truth that a few simple habits do almost all the work.

CHAPTER 1

A Note from Bill

Hello, and welcome. If the words "online security" make your shoulders tense up, you're in exactly the right place — and you can relax them right now. I wrote this book to take a subject that's usually made to sound frightening and complicated, and turn it into something calm, clear, and genuinely doable. Because here's the secret the headlines never tell you: protecting yourself online isn't about being clever or technical. It's about a few good habits, repeated.

I'm Bill. Helping folks feel at home and safe with their technology is what I do every day, and I'll walk you through this the way I'd sit beside you at your kitchen table: patiently, in plain English, with no scare tactics and no jargon. If I use a term you don't know, I'll stop and explain it on the spot.

What this book promises

By the end, you'll understand how to build strong passwords without memorizing a hundred of them, how to add a simple second lock to your most important accounts, how to spot the tricks scammers use, and what to do if something ever does go wrong. None of it is hard. All of it is worth it. And you can do every bit at your own pace.

WHAT THIS DOES FOR YOU

What good security really buys you

Security isn't about living in fear — it's the opposite. When your accounts are well protected, you stop worrying every time you shop online, check your email, or get a strange message. You can enjoy the conveniences of modern life — staying close to family, managing your money, shopping from your chair — without the nagging dread. That peace of mind is the whole point, and it's very much within your reach.

And I'm only a phone call away

This book will carry you a long way. But security is one area where it's especially smart to ask for help when you're unsure — and you never have to face it alone. Call me at **(330) 200-8042** and we'll sort it out together, with no judgment and no rush. Especially if you ever think something's gone wrong: the sooner we talk, the more we can protect. Now let's make you a hard target.

— Bill

CHAPTER 2

What "Securing Your Accounts" Means

Let's start simply. An **account** is any service you sign in to — your email, your bank, Amazon, Facebook, your pharmacy, Netflix. Each one holds something worth protecting: your money, your messages, your personal details, or simply your good name. **Securing** them means making sure only *you* can get in, and that a thief or scammer can't.

The three things we're protecting against

- **Someone guessing or stealing your password** and signing in as you.
- **Someone tricking you** into handing over your password or codes (this is the most common by far, and the one good habits guard against best).
- **Losing access yourself** — getting locked out of your own account because you forgot a password or lost a phone.

Everything in this book is aimed at these three. And the wonderful news is that the same few habits protect against all of them at once.

Not all accounts are equal

Some accounts matter far more than others. If someone broke into your crossword-puzzle app, you'd shrug. If they broke into your **email** or your **bank**, that's serious. So we'll spend our energy where it counts — protecting the few accounts that really matter most — rather than fretting equally over every little login. Working smart beats working hard.

GOOD TO KNOW

Your email is the master key — remember this

Here's the single most important idea in this whole book, so I'll plant it early: your **email account** is the master key to your digital life. Nearly every other account can be reset through your email ("forgot password? we'll email you a link"). So if a thief controls your email, they can walk into everything else. Protect your email above all — we'll give it its own chapter later.

CHAPTER 3

How Accounts Actually Get Broken Into

To protect yourself, it helps to know how the trouble actually happens — not the dramatic movie version, but the real, ordinary ways people lose control of their accounts. There are really only a few, and none of them is mysterious.

How it happens	What it looks like
Password reuse	You use the same password on many sites. One site gets breached, and now criminals try that same password everywhere — and get into your other accounts. Extremely common.
Weak, guessable passwords	Short or obvious passwords (a name, "123456," a birthday) can be guessed or cracked by computers in moments.
Phishing (being tricked)	A fake email, text, or website fools you into typing your password or a code. This is how most ordinary people actually get caught.
A leaked password from a company	A company you use gets hacked and your password leaks. If you reused it elsewhere, that's where the damage spreads.
A scammer on the phone	Someone calls, earns your trust or scares you, and talks you into sharing a code or password, or installing something.

Notice what's *not* on this list: some genius hacker targeting you personally through sheer technical wizardry. That's the movies. In real life, nearly everyone who loses an account does so through one of the everyday paths above — and every one of them is blocked by the simple habits in this book.

WHAT THIS DOES FOR YOU

Ordinary problems have ordinary solutions

Because account break-ins happen in a few predictable ways, defending against them is predictable too. You don't need to outsmart a master criminal — you just need to not reuse passwords, add a second lock to key accounts, and learn to recognize the tricks. That's it. The problem is smaller and more manageable than the fear around it suggests.

CHAPTER 4

The Few Habits That Do Most of the Work

Before we dig into the details, let me give you the whole book in a nutshell — the handful of habits that, together, protect you against the great majority of trouble. Everything that follows simply explains how to do each one. If you did nothing but these, you'd already be far safer than most people online.

The short list

1. **Use a different, strong password for every important account** (a password manager makes this effortless — Part 2).
2. **Turn on two-step verification** (a second lock) for your key accounts, especially email and bank (Part 3).
3. **Learn to recognize phishing** — the fake messages and sites that try to trick you (Part 4).
4. **Protect your email above all**, since it's the master key (Part 5).
5. **Know what to do if something goes wrong**, and act fast (Part 6).

You don't have to do it all today

Please don't feel you must overhaul everything this afternoon. Security is built one habit at a time. Start with your email, then your bank, then work outward as you're comfortable. Each small step makes you meaningfully safer, and there's no deadline. Progress, not perfection, is the goal here.

> **TIP**
>
> **Start with the two accounts that matter most**
>
> If this book ever feels like a lot, here's where to begin: give your **email** and your **bank** a strong, unique password and turn on two-step verification for each. Those two accounts protect the most — your identity and your money — and securing just them puts you ahead of most people. Everything else you can add at your leisure. One step at a time.

PART 2

Strong Passwords & Password Managers

What actually makes a password strong, why reusing passwords is the biggest everyday danger, and how a password manager makes doing it right completely effortless.

CHAPTER 5

What Makes a Password Strong

A password is the key to an account, and like a real key, some are far harder to copy than others. Let's clear up what actually makes a password strong — because a lot of the old advice turns out to be less useful than people think.

Length beats complexity

For years people were told to make passwords with a jumble of symbols, like "P@ssw0rd!". It turns out that what matters most is **length**, not fancy symbols. A longer password is dramatically harder for a computer to crack. The best passwords today are often a string of several unrelated words — something like *"copper-lantern-garden-quiet"* — which is both long (strong) and much easier to remember than a jumble of symbols.

What makes a password weak

- **Too short** — anything under about twelve characters is easier to crack.
- **Obvious** — your name, your pet's name, your birthday, your town, "password," "123456." All easily guessed.
- **A single common word**, or a word with a few numbers tacked on.
- **Reused** from another account (the biggest danger of all — next chapter).

What makes a password strong

- **Long** — twelve characters at the very least, and more is better. A few random words strung together works beautifully.
- **Unique** — used on only one account, nowhere else.
- **Unpredictable** — not based on information someone could learn about you.

GOOD TO KNOW

A "passphrase" is strong and memorable

Instead of a password, think **passphrase**: four or five random words together, like *"velvet-otter-mailbox-thunder."* It's long enough to be very strong, yet you can actually picture it and remember it. Pick words with no connection to each other or to you. This single idea — length through random words — is one of the most useful things in this book, especially for the few passwords you'll want to remember yourself.

CHAPTER 6

The Reuse Trap

If I could fix just one security habit for everyone, it would be this one — because reusing the same password across many accounts is, by a wide margin, the most common way ordinary people get into trouble. Let me show you exactly why, because once you see it, you'll never want to reuse a password again.

Why reuse is so dangerous

Companies get hacked — even big, careful ones — and sometimes their users' passwords leak out. When that happens, criminals take those leaked email-and-password pairs and **try them everywhere else**: your bank, your email, your shopping accounts. If you used the same password on those sites, the thieves walk right in — not because they're clever, but because you handed them the same key for every door.

The lightbulb example

Imagine you use one house key for your front door, your car, your safe deposit box, and your office. Lose that one key, or have it copied once, and a thief now has access to everything you own. That's exactly what reusing a password does. A different key for each lock means a single loss stays small. That's the whole case for unique passwords, in a nutshell.

HEADS UP

"But I can't remember a different password for everything!"

You're absolutely right — and you shouldn't have to. Nobody can remember dozens of strong, unique passwords, and trying to is why people reuse them. The answer isn't a better memory; it's a **password manager** — a simple tool that remembers them all for you, so you only have to remember one. That's the very next chapter, and it changes everything. Don't give up on unique passwords — just let a tool carry the load.

CHAPTER 7

Password Managers Explained

A **password manager** is the single most powerful tool for your online safety, and yet most folks have never used one. Let me demystify it, because it solves the impossible-memory problem completely and makes strong, unique passwords effortless.

What a password manager is

Think of it as a **locked safe for all your passwords**, kept on your phone and computer. It remembers a different strong password for every account, fills them in for you automatically when you sign in, and even creates new strong passwords when you need them. You unlock the safe with **one** master password (or your fingerprint or face), and it takes care of the rest.

What it does for you, day to day

- **Remembers every password** so you don't have to — you only remember the one that unlocks it.
- **Fills in logins automatically**, so signing in is often faster than typing.
- **Creates strong, unique passwords** at the tap of a button.
- **Warns you** if a password is weak, reused, or caught in a known leak.
- **Syncs across your devices**, so your passwords are with you on phone and computer alike.

GOOD TO KNOW

You may already have one built in

Both Apple and Google now include a password manager built into your phone and computer — Apple's **Passwords** app and **Google Password Manager** — and your web browser likely offers to save passwords too. There are also well-regarded standalone ones. You don't need anything fancy to start; the built-in tools are a fine, free beginning. The important thing is simply to *use* one.

Is it safe to keep all my passwords in one place?

It's a fair question, and the answer is yes — reputable password managers protect your passwords with strong encryption, so even the company can't read them, and the safe is locked behind your master password. The small risk of using one is far, far outweighed by the huge risk of the alternative: reused and weak passwords scattered everywhere. On

balance, a password manager makes you dramatically safer.

CHAPTER 8

Setting Up a Password Manager

Getting started is easier than you'd expect, and you can do it gradually — you don't have to move every password in one sitting. Here's the gentle way to begin.

Choosing one

For most folks, the simplest start is the one **already built into your device**: Apple's Passwords app on an iPhone, iPad, or Mac; Google Password Manager on an Android phone or in the Chrome browser. They're free, already there, and sync across your devices. If you'd like one that works everywhere regardless of device, there are trusted standalone managers too — a good thing to ask me about for a recommendation that fits you.

Your master password — the one you must remember

The password manager is locked by one **master password**. This is the one password you'll want to make truly strong and truly memorable — a long passphrase of random words (Chapter 5) is perfect. Because it unlocks everything, never reuse it anywhere else, and write it down on paper kept somewhere safe and private at home, in case you forget.

Starting gradually

1. Turn on the password manager and set your master password (or let it use your fingerprint or face to unlock).
2. As you sign in to your accounts over the coming days, let it **offer to save** each password.
3. For your most important accounts — email and bank first — use it to create a **new strong, unique password**, replacing any you've reused.
4. Over a few weeks, it fills up naturally. No need to rush the whole list at once.

> **TIP**
>
> **Let it fix your worst passwords first**
>
> A good password manager can show you which of your passwords are weak or reused. Start there: fix the handful that are reused on important accounts, and you've removed most of your risk in an afternoon. You don't have to achieve a perfect list — just knock out the dangerous reuses on the accounts that matter, and let the rest improve over time.

CHAPTER 9

Using a Password Manager Day to Day

Once it's set up, a password manager mostly works quietly in the background and makes your life *easier*, not harder. Here's what using it feels like in everyday life.

Signing in

When you go to sign in to a website or app, the password manager recognizes it and offers to fill in your username and password — usually you just tap it or confirm with your fingerprint or face, and you're in. No typing, no remembering. It's often quicker than doing it by hand.

Making a new account

When you sign up for something new, the manager offers to **create a strong password** for you and saves it automatically. You never have to think one up or remember it — it's handled. This is how unique passwords become effortless: the tool does the work.

Finding a password when you need it

If you ever need to see a password — to sign in on a different device, say — you can open the password manager, unlock it, and look it up. Everything's in one searchable place, which is far tidier and safer than sticky notes or a scattered notebook.

WHAT THIS DOES FOR YOU

Stronger security that's also less work

Here's the lovely surprise about password managers: they make you much safer *and* make your daily life easier. No more forgotten passwords, no more resetting them, no more typing. It's one of the rare cases where the safe choice is also the convenient one. Once you've used one for a week, you'll wonder how you ever managed without it.

CHAPTER 10

Writing Passwords Down — the Safe Way

Maybe a password manager feels like a step too far right now, or maybe you just want a backup for your most important passwords. That's fine — and writing passwords down on paper is perfectly reasonable, as long as you do it sensibly. Let's do it the safe way.

The sensible rules

- **Use a dedicated notebook** kept in a private, secure spot at home — a drawer, a safe, somewhere only you and perhaps your closest family know.
- **Don't label it "Passwords"** in big letters, and don't stick passwords to your computer or under the keyboard.
- **Still use different passwords** for each account — the notebook is what lets you, since you don't have to memorize them.
- **Keep it updated** and note which account each one is for.
- **Never carry it with you** or keep it in your wallet or purse.

Paper vs. a password manager

A notebook at home is far better than reusing one password everywhere — so if that's your starting point, good. Its limits are that it doesn't fill passwords in for you, doesn't warn you about leaks, and isn't with you when you're out. A password manager does all that. Many people happily use both: the manager for everyday use, and a written list of their few most critical passwords locked away as a backup.

STAY SAFE

Never share your written list over the phone or email

Whether your passwords live in a notebook or a manager, the rule is the same: **no one legitimate will ever ask you to read them out**. Not your bank, not "support," not a caller, not an email. Anyone asking for your passwords is trying to rob you. Your list is for your eyes only — keep it that way, and the scammers have nothing to work with.

PART 3

The Second Lock: Two-Step Verification

The single most powerful thing you can do after good passwords: adding a second lock so a stolen password alone isn't enough to get into your accounts.

CHAPTER 11

What Two-Step Verification Is

If strong passwords are the first lock on your door, **two-step verification** is a second, different lock — and it's so effective that turning it on for your important accounts is one of the best things you'll ever do for your safety. You'll see it called a few names; they all mean the same thing.

The names all mean the same thing

Two-step verification, **two-factor authentication**, **2FA**, **2-step verification**, **multi-factor authentication** — don't let the jumble of names throw you. They all describe the same simple idea: after you type your password, the account asks for *one more thing* to prove it's really you — usually a short code, a tap on your phone, or your fingerprint or face.

Why it's so powerful

Here's the magic of it: even if a thief somehow gets your password — guessed it, found it in a leak, or tricked you — they **still can't get in**, because they don't have your phone to receive that second step. It turns a stolen password from a disaster into a harmless scrap. One simple feature closes the door on the great majority of account break-ins.

WHAT THIS DOES FOR YOU

The best half-hour you'll spend on your safety

Turning on two-step verification for your email and bank takes maybe half an hour total, once, and it protects you against most of the ways accounts get stolen — for years to come. If you do only one thing from this entire book beyond not reusing passwords, make it this. It's the closest thing to a magic shield that online safety offers.

The one small trade-off

The honest downside is tiny: signing in takes a few extra seconds, since you provide that second step. For your important accounts, that mild inconvenience is a wonderful bargain for the protection it buys. And on your own trusted devices, many accounts only ask for the second step occasionally, not every single time.

CHAPTER 12

The Three Kinds of Second Step

The "second step" can take a few forms, and they're not all equally strong. Here's the plain ranking, worst to best, so you know what you're using and what to prefer. The good news: any of them is vastly better than none.

Kind	What to know
Text-message code (SMS)	A code texted to your phone. The most common and the easiest to set up — and far better than nothing — but the weakest of the three, since texts can occasionally be intercepted or redirected.
Authenticator app	A free app on your phone that generates a fresh code every 30 seconds. Stronger than texts, because nothing is sent that could be intercepted.
Passkey	The newest and strongest: your fingerprint or face unlocks the account, with nothing to type and nothing a fake site can steal. The best option where it's offered.

We'll look at each in turn. If choosing feels like too much, here's the simple takeaway: **turn on whatever your account offers** — even text codes — and prefer an authenticator app or a passkey when it's easy. Something is enormously better than nothing.

GOOD TO KNOW

Don't let "which is best" stop you from turning on "good"

People sometimes get so tangled in picking the *best* second step that they never turn on *any*. Don't fall into that trap. A text-message code is far, far better than no second step at all. Turn on whatever's easiest today; you can always upgrade to an app or passkey later. The worst choice is leaving the second lock off entirely.

CHAPTER 13

Text-Message Codes

The most common second step is a **code sent by text message** to your phone. You type your password, the account texts you a short number, you type that number in, and you're verified. It's simple, familiar, and a fine place to start.

How it works

1. You sign in with your password as usual.
2. The account sends a text to your phone with a short code (say, six digits).
3. You type that code into the sign-in screen.
4. You're in — and the thief who has only your password is left out.

Its one weakness

Text codes have a known soft spot: in rare, targeted cases, criminals can trick a phone company into moving your number to their phone (so the codes go to them), or intercept a text. This is uncommon and usually aimed at specific high-value targets — but it's why experts rank texts below apps and passkeys. For most everyday accounts, text codes are still a big improvement; for your most sensitive accounts, prefer an app or passkey if you can.

STAY SAFE

Never, ever read a code aloud to someone who contacts you

This bears repeating because it's how many people are robbed: a scammer calls or texts, often pretending to be your bank or a company, and asks you to tell them the code you just received. **Never do it.** That code is the key to your account, and they're trying to use it that very second. No legitimate company will ever ask you to read a verification code to them. If anyone does, it's a scam — hang up.

CHAPTER 14

Authenticator Apps

A step up from text codes is an **authenticator app** — a free app on your phone that generates its own codes. It sounds technical, but it's genuinely simple to use once set up, and it's stronger than texts because nothing is sent through the phone network to be intercepted.

How it works

The app shows a six-digit code that changes every thirty seconds, like a little rolling combination lock. When an account asks for your second step, you open the app, read the current code, and type it in. Because the code is generated right on your phone and never sent anywhere, there's nothing for a criminal to intercept.

Common authenticator apps

Popular free ones include **Google Authenticator**, **Microsoft Authenticator**, and the authenticator built into some password managers. Your phone (Apple or Google) may also offer this built in. Any reputable one is fine; you don't need more than one.

> **TIP**
>
> **Set up a backup when you use an authenticator app**
>
> The one thing to plan for with an authenticator app: what happens if you lose or replace your phone? Many apps now back up to your account or let you move them to a new phone, and accounts give you **backup codes** (Chapter 16) for exactly this. When you set up an authenticator, save those backup codes somewhere safe so a new phone never locks you out. This is a great thing to set up together on a call if you'd like.

CHAPTER 15

Passkeys — the New Best Way

The newest and strongest way to sign in is the **passkey**, and it's quietly becoming available on more and more accounts. It's worth understanding, because it's both the most secure option *and* often the easiest to use — a rare and welcome combination.

What a passkey is

A passkey lets you sign in using the same **fingerprint, face, or PIN** that unlocks your phone or computer — with no password to type at all. Behind the scenes, your device proves who you are to the account without ever sending a password or code that could be stolen. You just glance at your phone or touch the sensor, and you're in.

Why it's so secure

Because there's no password or code to type, there's nothing for a fake website to trick out of you and nothing to intercept. Passkeys are, by design, **resistant to phishing** — they simply won't work on a fake look-alike site. That makes them the strongest everyday protection available, and they're easier than remembering anything.

GOOD TO KNOW

Try a passkey when an account offers one

When you sign in somewhere and it asks "Create a passkey?" or "Sign in faster with a passkey?", it's worth saying yes on your own trusted phone or computer — especially for big accounts like Google, Apple, Microsoft, and major banks. Your password usually still works as a backup. Passkeys are new, so you won't see them everywhere yet, but they're the direction everything is heading, and they're a pleasure to use.

CHAPTER 16

Turning It On, and Backup Codes

Let's make this practical. Turning on two-step verification is done in each account's settings, and the shape is the same everywhere once you've seen it. We'll also cover the all-important backup codes that keep you from ever locking yourself out.

Where to find it

In almost any account, look in **Settings** for a section called **Security** (sometimes "Sign-in & security" or "Password & security"). There you'll find **Two-Step Verification** or **Two-Factor Authentication**. Turn it on, and the account walks you through choosing your second step — a text code, an app, or a passkey.

The general steps

1. Sign in to the account and open **Settings > Security**.
2. Find and choose **Two-Step (or Two-Factor) Verification** and turn it on.
3. Pick your second step: phone text, authenticator app, or passkey.
4. Follow the prompts to confirm it (you'll usually test it once).
5. **Save the backup codes** it offers — see below.

Backup codes: your spare key

When you turn on two-step verification, most accounts give you a set of **backup codes** — a short list of one-time codes to use if you ever can't get your normal second step (you've lost your phone, say). **Save these.** Print them or write them down and keep them with your important papers at home. They're the spare key that prevents the one real downside of two-step verification: locking yourself out.

HEADS UP

Set up two-step on a calm day, not in a panic

Turn on two-step verification when you have a quiet few minutes and your phone in hand — not when you're rushing or stressed. That way you can test it, save your backup codes properly, and make sure everything works smoothly. Do your email first, then your bank, then others over time. And if any account's setup confuses you, that's a perfect thing to do together — call me and we'll walk through it.

PART 4

Recognizing the Tricks

Most people who lose an account aren't hacked — they're tricked. Here's how to spot the fake messages, fake sites, and scam calls before they catch you.

CHAPTER 17

Phishing: the Fake-Message Trick

The number-one way ordinary people lose control of their accounts isn't fancy hacking — it's being **tricked** into handing over their own password or code. This trickery has a name: **phishing** (said "fishing," and that's exactly the idea — dangling bait and hoping you bite). Learn to recognize it and you've closed the biggest door of all.

How phishing works

A scammer sends you a message — an email, a text, sometimes a phone call — dressed up to look like it's from someone you trust: your bank, Amazon, Apple, Microsoft, the post office, even a friend. It creates a reason for you to act, and steers you to type your password or a code into a fake page, or to call a fake number, or to hand over personal details. You think you're dealing with the real company; you're really handing the keys to a thief.

The usual bait

- "There's a problem with your account — sign in to fix it."
- "Your package couldn't be delivered — confirm your details."
- "Suspicious activity detected — verify it was you."
- "You've won / you're owed a refund — claim it here."
- "Your payment failed — update your card."

SCAM ALERT

The golden rule that defeats phishing

Here's the one habit that beats nearly all phishing: **never sign in, pay, or share details through a link someone sent you.** Instead, go to the company yourself — type their address into your browser, or use the app or phone number you already have. If the "problem" is real, you'll see it when you log in the normal way. If it's not there, it was bait. This single rule protects you from the great majority of online fraud.

CHAPTER 18

Spotting a Phishing Email or Text

Phishing messages have tells — little signs that give them away once you know to look. None is foolproof alone, but together they light up a fake like a warning sign. Here's what to watch for.

Warning sign	What it means
A sense of urgency or threat	"Act now or your account will be closed!" Real companies rarely pressure you like this. Urgency is the scammer's favorite tool.
A link that wants you to sign in	Any message pushing you to click and log in should make you suspicious. Go to the site yourself instead.
Slightly-wrong sender or web address	Look closely: "amaz0n-support.com" or an odd address. Fakes are often *almost* right.
Generic greeting	"Dear Customer" or "Dear User" instead of your name can be a sign — though scammers sometimes know your name too.
Spelling and odd phrasing	Clumsy grammar or strange wording often (not always) marks a fake.
Unexpected attachments	A bill, receipt, or "document" you didn't expect — don't open it.

TIP

When in doubt, slow down and check another way

You never have to decide in the moment. If a message about an account gives you even a flicker of doubt, set it aside and check *independently*: call the company using the number on your card or statement, or sign in to their real site yourself. A genuine issue will still be there; a scam falls apart the moment you check through a channel the scammer doesn't control.

CHAPTER 19

Fake Login Pages & Websites

A favorite phishing trick is the **fake login page** — a web page built to look exactly like your bank's or email provider's sign-in screen. You type your password; it goes straight to the thief. These can be remarkably convincing, so let's learn to see through them.

How to tell a fake from the real thing

- **Check the web address** at the very top of the browser. The real site has the company's exact address (like *chase.com*); fakes use look-alikes (*chase-secure-login.com*) or odd endings. Read it carefully.
- **You arrived by clicking a link?** That's the red flag. You should reach a login page by typing the address or using your saved bookmark — not from an email or text link.
- **A password manager that won't fill in** is a quiet clue: it recognizes the *real* site and won't offer your password on a fake one. If it doesn't auto-fill where it normally would, be suspicious.

GOOD TO KNOW

A password manager quietly protects you from fake sites

Here's a hidden benefit of using a password manager: it ties each saved password to the *real* website's address. On a fake look-alike site, it simply won't offer to fill your password in — because it knows this isn't the real place. That silent "hmm, it's not filling in" moment has saved many people from a convincing fake. One more reason to use one.

The safest habit of all

Bookmark the real sign-in pages for your important accounts — your bank, your email — and reach them only through those bookmarks or by typing the address yourself. If you never sign in by clicking a link in a message, fake login pages simply can't catch you. It's a small habit with enormous protective power.

CHAPTER 20

Scam Phone Calls & "Tech Support"

Not all attacks come by message — many come by **phone**, and these can be especially convincing because a real voice, calm and authoritative, is persuasive. Phone scams aimed at older folks are sadly common, so let's arm you against them.

The common phone scams

- **"Tech support"** — someone claims your computer is infected or your account is hacked, and offers to "help" if you let them connect to your computer or share a code. Always a scam.
- **"Your bank's fraud department"** — a caller says there's fraud on your account and, to "protect" you, needs your password, a code, or for you to move money. Real banks don't do this.
- **"A company you use"** — Amazon, Apple, Microsoft, calling about a charge or problem and asking for access or payment.

SCAM ALERT

Real companies don't call you and ask for access or codes

Burn this into memory: **no real bank, tech company, or government agency will call you out of the blue and ask for your password, a verification code, remote access to your computer, or for you to move your money.** Those are the scammer's demands, every time. If you get such a call, hang up — even if the caller ID looks official (it can be faked). Then, if you're worried, call the company yourself using the number on your card or statement. And if it's about your computer, call me first — **(330) 200-8042**.

Don't trust caller ID

Scammers can make your phone's caller ID show any name or number they like — your bank's name, a government agency, even a local number. So the name on the screen proves nothing. Judge a call by what the caller *asks you to do*, not by what the caller ID says. If they want codes, passwords, access, or money, it's a scam no matter whose name appears.

CHAPTER 21

Urgency, Fear & Too-Good-to-Be-True

Underneath every scam, whatever its disguise, are the same few emotional tricks. Learn to feel these levers being pulled and you'll recognize a scam even in a form you've never seen before. The *feeling* is the tell.

The emotional levers scammers pull

The lever	How it's used
Urgency	"Act now! Only minutes left! Your account closes today!" Rushing you stops you thinking and checking. Real matters give you time.
Fear	Threats of arrest, lost money, a hacked account, trouble with the law. Fear makes people obey without questioning.
Too good to be true	A prize, a refund, an inheritance, a sweetheart deal. If it seems too good to be true, it is.
Secrecy	"Don't tell anyone" / "don't discuss this with your bank or family." Isolation is how they keep you from being talked out of it.
Authority	Posing as your bank, the government, a big company — to borrow trust they haven't earned.

TIP

Strong feelings are a signal to slow down

Here's a wonderful rule of thumb: whenever a message or call makes you suddenly feel **afraid, rushed, or thrilled**, treat that feeling itself as a warning to *slow down*, not speed up. Those emotions are exactly what scammers manufacture to short-circuit your good judgment. The moment you notice them, stop, breathe, and check with someone you trust. Calm is the scammer's enemy.

CHAPTER 22

Links & Attachments: Look Before You Click

So much of staying safe comes down to a single moment: the instant before you click a link or open an attachment. A little care in that moment prevents a great deal of trouble. Let's build the habit.

Before you click a link

- **Ask: was I expecting this?** An unexpected link, even from someone you know, deserves a second thought (their account may be hacked).
- **Don't sign in or pay through it.** If a link leads to a login or payment page, go to the site yourself instead (Chapter 17).
- **Hover to see where it really goes** — on a computer, rest the mouse over a link (without clicking) and the true address appears; if it's not what you'd expect, don't click.

Before you open an attachment

- **Were you expecting a file from this person?** If not, don't open it — confirm with them first, another way.
- **Be wary of "invoices," "receipts," "documents," and "voicemails"** you didn't expect — a favorite way to deliver harmful files.
- **When unsure, don't** — and ask me. An unopened attachment can't hurt you.

STAY SAFE

The pause that protects you

You don't need technical skill to stay safe — you need a two-second pause. Before every click on a link or attachment, just ask: *"Was I expecting this, and does it want me to sign in, pay, or open something?"* That tiny habit, done faithfully, stops most online attacks cold. When the answer gives you pause, trust it — and call me if you'd like a second opinion before you click.

PART 5

Protecting Your Key Accounts

Where to focus your effort: your email above all, then your bank, your shopping and social accounts, and the phone that ties it all together.

CHAPTER 23

Your Email: the Master Key

We've mentioned it a few times, and now it gets its own chapter because it's that important: your **email account** is the master key to your entire online life. Protect it above everything else, and you've protected most of what matters.

Why email is the master key

Think about what happens when you forget a password on almost any website. You click "forgot password," and the site emails you a link to reset it. That's wonderfully convenient — but it means that **whoever controls your email can reset the passwords to your other accounts**: your bank, your shopping, your social media. Your email is the skeleton key that opens everything else. A thief who gets into it can take over your whole digital life from there.

What this means for you

It means your email deserves your *strongest* protection: a long, unique password that you use nowhere else, and two-step verification turned on without fail. If you do that for no other account, do it for your email. Everything else depends on it.

WHAT THIS DOES FOR YOU

Secure the master key, protect the whole house

There's something reassuring about this: because so much flows through your email, securing that *one* account does an outsized amount of good. A strong, unique password plus two-step verification on your email is perhaps the single highest-value thing you can do for your online safety. One account, well guarded, protects the rest.

CHAPTER 24

Locking Down Your Email

Let's make your email as safe as it deserves to be. Whether you use Gmail, Outlook, Yahoo, AOL, or another, the steps are the same in spirit, and none takes long.

The email security checklist

1. **Give it a strong, unique password** — a long passphrase used nowhere else (Chapter 5).
2. **Turn on two-step verification** — this is the big one for email (Chapter 16).
3. **Save your backup codes** somewhere safe, in case you lose your phone.
4. **Check your recovery details** — make sure the backup phone number and recovery email on the account are current and yours, so you can always get back in.
5. **Review recent activity** if your email offers it — a "recent sign-ins" or "security" page shows where it's been accessed, so you can spot anything strange.

Watch for sneaky changes

If a thief ever does get into an email account, a common trick is to set up a hidden **forwarding rule** that secretly sends copies of your messages to them, or to change your recovery details. Once in a while, glance at your email's settings for any forwarding you didn't set up, and confirm your recovery phone and email are still yours. It's a quick check that catches a sneaky intruder.

> **TIP**
>
> **Do this one today if you do nothing else**
>
> If this chapter is the only one you act on this week, you've spent your time wisely. Give your email a strong unique password and switch on two-step verification, and you've locked the most important door in your digital house. Put the kettle on, set aside twenty quiet minutes, and knock it out — or call me and we'll do it together. It's that worthwhile.

CHAPTER 25

Your Bank & Financial Accounts

After your email, your **bank and financial accounts** are what deserve the most care — they're where the money is, and the most direct target. The good news is that banks take security seriously and give you strong tools; you just have to use them.

Securing your financial accounts

- **Strong, unique passwords** for each — never the same password as another site.
- **Two-step verification turned on** — prefer an authenticator app or passkey here if offered, but any second step is good.
- **Turn on account alerts** — most banks can text or email you when money moves, so you spot anything wrong immediately.
- **Use the official app or typed web address** — never reach your bank through a link in a message.

Check your statements

One of the oldest and best protections still works: **read your statements**, or glance at your account online, regularly. Unfamiliar charges — even small ones — can be the first sign of trouble, and catching them early makes them far easier to undo. If you see something you don't recognize, contact your bank using the number on your card, not any number from a message.

SCAM ALERT

Your bank will never ask you to "move money to keep it safe"

A particularly nasty scam has a "bank fraud department" call to say your account is compromised and you must move your money to a "safe account" they provide — or share codes to "protect" it. This is **always** a scam; the "safe account" is the thief's. Real banks never ask you to move money this way or share codes. If you get such a call, hang up and call your bank yourself using the number on your card. When in doubt, call me first.

CHAPTER 26

Shopping & Everyday Accounts

Shopping accounts like Amazon, along with your other everyday logins, matter too — they often have your card saved and your address on file, which a thief would love. They don't need quite the fortress your email and bank do, but they're worth a sensible level of care.

Sensible protection for shopping accounts

- **A unique password** (your password manager makes this painless).
- **Two-step verification** where offered — easy to turn on and well worth it for an account with your card saved.
- **Watch your order history and card statements** for purchases you didn't make.
- **Be cautious about saving your card** on sites you rarely use — fewer places holding your card means fewer places it can leak from.

SCAM ALERT

Beware fake "order problem" and "delivery" messages

Because so many of us shop and expect packages, scammers flood inboxes and phones with fake "there's a problem with your order" and "your package is held — confirm your details" messages. They lead to fake login or payment pages. Don't click. To check a real order, go to the store's app or type its address yourself and look at your orders there. If there's truly a problem, you'll see it; if not, it was bait.

CHAPTER 27

Social Media Accounts

Social media — Facebook, Instagram, and the rest — is where many of us stay close to family and friends, which is exactly why it's worth protecting. A hijacked social account is often used to scam the very people you care about, by impersonating you.

Protecting your social accounts

- **A unique password** and **two-step verification**, same as everywhere.
- **Be thoughtful about what you share publicly** — details like your birthday, hometown, and pets' names can help someone guess passwords or answer security questions.
- **Review privacy settings** so your posts go to friends, not the whole world, if that's your preference.

SCAM ALERT

If a "friend" messages asking for money or codes, it may not be them

A very common scam: your account (or a friend's) gets taken over, and the thief messages that person's friends — "I'm in trouble, send money" or "can you receive a code for me?" Because it comes from a real account, people trust it. If a friend or family member messages with an urgent request for money, gift cards, or codes, **check by calling them directly** before doing anything. And never share a verification code on someone else's behalf — that's a trick to hijack *your* account.

If your social account gets taken over

Each platform has a "forgot password" and account-recovery process to help you regain a hijacked account — we'll talk about recovery generally in Part 6. The key is to act quickly, warn your friends not to trust messages from the account until you're back in control, and change your password and turn on two-step verification once you recover it.

CHAPTER 28

Your Phone, Its Lock & Device Accounts

Your phone deserves special mention, because it's become the hub of your digital life — it receives your verification codes, holds your email and apps, and often your password manager. Protecting the phone itself is part of protecting everything on it.

Locking your phone

- **Use a screen lock** — a PIN, fingerprint, or face. A phone with no lock is an open door to everything inside if it's lost or stolen.
- **Make the PIN not obvious** — not "0000," "1234," or your birth year.
- **Set it to lock quickly** when idle, so it isn't sitting unlocked if you set it down.

Your device account (Apple or Google)

Your phone is tied to a big account — an **Apple Account** on an iPhone, or a **Google account** on an Android phone. This account is a master key in its own right (it can locate, lock, or erase your phone, and holds a lot of your information), so give it a strong unique password and two-step verification, just like your email.

TIP

Set up "find my phone" — it's a lifesaver

Both Apple and Google let you locate, lock, and even erase your phone remotely if it's lost or stolen — **Find My** on an iPhone, **Find My Device** on Android. Turn it on now, while your phone is in your hand. If the day ever comes that your phone goes missing, you'll be enormously glad you did — you can lock it from afar so no one can get at what's inside. A wonderful bit of insurance that costs nothing.

PART 6

If Something Goes Wrong

Even careful people sometimes run into trouble. Here's how to spot it early, act fast, recover your accounts, and keep calm through it all.

CHAPTER 29

Signs Something May Be Wrong

Catching trouble early makes it far easier to fix. Here are the signs that one of your accounts may have been compromised. If you notice any, don't panic — just act promptly using the steps in the chapters that follow.

Warning signs to watch for

- You're **locked out** of an account that worked yesterday, or your password suddenly "doesn't work."
- You get **emails or texts about changes you didn't make** — a password reset, a new login, a changed recovery number.
- **Friends say they got strange messages from you** that you never sent.
- You see **purchases, posts, or messages you didn't make**.
- Your **email has sent items or forwarding rules** you don't recognize.
- A **verification code arrives** when you weren't trying to sign in (someone may be trying to get into your account right then).

HEADS UP

An unexpected code means someone's at the door — don't let them in

If you receive a verification code you didn't request, it usually means someone has your password and is trying to get in *at that moment* — and the only thing stopping them is that second step they don't have. **Do not share that code with anyone**, and don't type it anywhere. Instead, treat it as a signal to change that account's password soon, because someone knows it. If it keeps happening, call me and we'll secure things properly.

CHAPTER 30

What to Do If an Account Is Hacked

If an account has been taken over, acting quickly and in the right order limits the damage and gets you back in control. Here's the plan. Keep this page handy — in a stressful moment, a clear checklist is a great comfort.

The steps, in order

1. **Change the password** on that account right away (if you can still get in). Make the new one strong and unique.
2. **Turn on two-step verification** if it wasn't already on — this kicks out an intruder who only has your old password.
3. **Change the password on any other account that used the same password** — this is why reuse is so dangerous.
4. **Check the account for the intruder's changes** — a changed recovery email or phone, forwarding rules, new "trusted" devices — and undo them.
5. **If it's a financial account**, contact the bank or card company using the number on your card.
6. **Warn affected people** — if a social or email account was used to message others, tell them not to trust recent messages.

FROM BILL

Hacked? Call me — we'll work the list together

Discovering an account has been hacked is upsetting, and it's easy to miss a step when you're rattled. Please call me at **(330) 200-8042** and we'll go through it calmly together, in the right order, making sure the intruder is fully locked out and nothing's overlooked. This is exactly the kind of moment I'm here for — no judgment, just steady help getting you back in control.

CHAPTER 31

Recovering a Locked-Out Account

Sometimes the problem isn't a hacker — it's simply that *you* can't get in: a forgotten password, a lost phone, a changed number. Every major service has ways to help you prove it's you and get back in. Don't despair, and don't hand the job to a stranger.

The usual recovery paths

- **"Forgot password"** — the first thing to try. It sends a reset to your recovery email or phone.
- **Backup codes** — if you saved them when turning on two-step verification (Chapter 16), now is when they shine.
- **Recovery email or phone** — the backup contacts you set on the account.
- **The service's account-recovery process** — a guided series of questions to prove your identity when the quick options don't work.

Why backups matter so much

This chapter is really an argument for setting up your recovery options *before* you need them — a current recovery email and phone, saved backup codes. People who set these up get back in quickly; people who didn't can face a long, frustrating process. If you take a moment now to make sure your important accounts have good recovery details, you'll thank yourself later.

SCAM ALERT

Beware fake "account recovery" helpers

When people are locked out and desperate, scammers pounce — offering "account recovery services," fake support numbers, or "helpers" who promise to get you back in for a fee or if you share your details. These are traps. Use only the **official** recovery process on the real service's site (reached by typing its address), or call me. Never pay a stranger or share your information with an unofficial "recovery" service.

CHAPTER 32

If Your Email Is Compromised

Because email is the master key, a compromised email account is the most serious case and deserves its own quick plan. If you suspect someone has gotten into your email, act fast — from there they could reach your other accounts.

Act in this order

1. **Change your email password** immediately to a new strong, unique one (if you can still get in).
2. **Turn on two-step verification** for the email if it wasn't on.
3. **Check for the intruder's tricks** — hidden forwarding rules, a changed recovery phone or email, new app connections — and remove them.
4. **Review your other important accounts** (bank, shopping) for any password resets the intruder may have triggered through your email, and secure them.
5. **Warn your contacts** if the account sent spam or scam messages in your name.

> FROM BILL
>
> **This is a 'call Bill right away' situation**
>
> A hacked email is serious enough that I'd rather you not face it alone. If you think someone has gotten into your email, call me at **(330) 200-8042** as soon as you can. We'll lock the intruder out, undo their sneaky changes, and check that they didn't use your email to reach anything else — calmly and thoroughly. The faster we act, the less harm done.

CHAPTER 33

Identity Theft: the Basics

Identity theft is when a criminal uses your personal information — your name, Social Security number, or financial details — to pretend to be you: opening accounts, taking loans, or filing for benefits in your name. It's frightening, but there are clear, official steps to limit the damage and recover, and you don't have to navigate them alone.

Signs of identity theft

- Bills or accounts you never opened, or collection calls for debts that aren't yours.
- Being turned down for credit unexpectedly, or notices of credit applications you didn't make.
- Tax or benefit problems suggesting someone filed using your information.

First steps if it happens

The U.S. government has an official, free resource that walks you through exactly what to do, step by step, and even generates a recovery plan — it's the authoritative place to start, and you can reach it by searching for the government's identity-theft help (a **.gov** site). Key early moves usually include contacting the affected companies, placing a fraud alert or freeze on your credit with the credit bureaus, and keeping careful records. It's a process, but a well-charted one.

FROM BILL

Don't face identity theft alone

Identity theft is overwhelming precisely because it touches so many accounts at once. If it happens to you, call me at **(330) 200-8042**. I can't be your lawyer or your bank, but I *can* help you reach the right official resources, work through the steps in order, secure your accounts and devices, and make sure you're not missing anything. Having a steady hand beside you makes a hard situation much more manageable.

CHAPTER 34

Keeping Calm & Acting Fast

If there's one message to carry out of this part of the book, it's this: if something goes wrong, **the worst thing is to freeze with worry or shame, and the best thing is to act promptly and get help**. Trouble caught early and handled calmly is usually very fixable.

The mindset that serves you

- **Don't blame yourself.** These criminals fool careful, intelligent people every day. Being targeted isn't a failing.
- **Act, don't agonize.** Speed limits damage far more than hindsight ever could.
- **Ask for help early.** A trusted person — family, your bank, me — makes everything easier and catches what you might miss.
- **Keep records** of what happened and what you did, in case you need them later.

WHAT THIS DOES FOR YOU

Prepared, not fearful

You've now learned not only how to protect your accounts but how to respond if something slips through. That's the complete picture — and it should leave you feeling *prepared*, not frightened. The vast majority of people who follow the habits in this book never face serious trouble, and those who do handle it far better for knowing the steps. You're ready either way.

PART 7

Habits, Answers & When to Call Bill

A simple routine to keep you safe for good, plain answers to the questions I hear most, and — honestly — when to let me lend a hand.

CHAPTER 35

Your Simple Security Routine

Good security isn't a one-time project — but it's also not a burden. A light routine keeps you protected with just a few minutes now and then. Here's an easy rhythm. Pin it up, and you'll stay a hard target without ever thinking hard about it.

When	What to do
Once, to get started	Give your email and bank strong, unique passwords and turn on two-step verification. Start a password manager. Save your backup codes.
Each time you sign up somewhere new	Let your password manager create and save a unique password. Turn on two-step verification if offered.
Monthly	Glance at your bank and card statements for anything you don't recognize.
Every few months	Let your password manager fix any weak or reused passwords it flags. Confirm your recovery email and phone are current on key accounts.
Any time something feels off	Don't act on a suspicious message — check independently, and call someone you trust.

WHAT THIS DOES FOR YOU

Small habits, lasting safety

This is the whole book in a routine: strong unique passwords (a manager makes it easy), two-step verification on what matters, a wary eye for tricks, and a quick check of your statements. None of it is hard, and together they protect you against nearly everything. A few minutes now and then buys you lasting peace of mind.

CHAPTER 36

Questions People Ask Me All the Time

The same good questions come up again and again. Here are my plain answers to the ones I hear most about staying safe online.

Isn't it dangerous to keep all my passwords in one app?

It feels that way, but a reputable password manager is far safer than the alternative — reused and weak passwords everywhere. Your passwords are strongly encrypted and locked behind your master password. The real danger isn't using a manager; it's *not* using one.

Do I really need two-step verification? It's a hassle.

Yes — it's the single most effective protection there is, and the "hassle" is a few extra seconds now and then. On your own trusted devices, many accounts only ask occasionally. For your email and bank especially, it's worth it many times over.

How often should I change my passwords?

The old advice to change them constantly is out of date. A **strong, unique** password doesn't need regular changing. Change a password when there's a reason: a breach, a suspicion, or because it's weak or reused. Energy is better spent making them unique and adding two-step verification than rotating them on a schedule.

Someone called from "Microsoft" / my bank. Was it real?

Almost certainly not. Real companies don't call out of the blue asking for passwords, codes, remote access, or for you to move money. Hang up, and if you're concerned, call the company yourself using the number on your card or statement — never a number the caller gives you.

Are passkeys safe? They seem too easy.

They're safe precisely *because* they're easy — there's no password or code for a fake site to steal, and they won't work on a look-alike site. When a major account offers a passkey on your own trusted device, it's a fine, strong choice.

I think I clicked a bad link. What now?

Don't panic. If you didn't type a password or details, you're likely fine — close the page. If you *did* enter a password, change it on that account right away (and anywhere you reused it), and turn on two-step verification. Then call me if you'd like a hand making sure all's well.

FROM BILL

Still have a question? Just ask

If your question isn't here, that's exactly what I'm for. There's no such thing as a silly question about staying safe, and I've helped many folks through every part of it. Call or text me at **(330) 200-8042** and we'll sort it out together.

CHAPTER 37

When to Call Bill

This book is meant to make you confident and safe online, and most of it you can handle on your own. But security is one area where asking for help early is especially wise — and you never have to face it alone. Here's when a call makes good sense.

Good reasons to call

- You'd like a hand setting up a password manager or turning on two-step verification for your important accounts.
- You got a message, call, or email and you're not sure if it's a scam — call me *before* you click, reply, pay, or share anything.
- You're locked out of an account and the recovery options aren't working.
- You think an account may have been hacked, or you may have been tricked — the sooner we act, the better.
- You fear you're a victim of identity theft and need help reaching the right official resources and working the steps.
- You simply want someone to review your setup and tell you honestly where you're exposed.

SCAM ALERT

The call I most want to get

Please hear this plainly: if anything online ever pressures you — to hurry, to pay, to share a password or a code, to let someone onto your computer — stop and call me first, at **(330) 200-8042**. There is never any shame in checking, and I would far rather answer a two-minute "is this real?" question than help someone recover afterward. Checking with me *is* the smart, safe move — never a bother.

How to reach me

I'm Bill, and I help folks right here in **Portage County, Ohio** with exactly this kind of thing. Call or text **(330) 200-8042**, or book a visit online at **billshometech.com/book**. If you call the main line and reach my assistant **Sophie**, she can answer simple questions and get you on my schedule — she's there to help. With 30+ years of professional experience, there's very little I haven't helped folks through, and no question too small to ask.

— Bill

CHAPTER 38

Your Account-Security Cheat-Sheet

Tear this page out, or fold the corner, and keep it handy. It's the whole book boiled down to what matters most.

The habits that protect almost everything

1. **A different, strong password for every important account** — let a password manager do the remembering.
2. **Two-step verification on your key accounts** — email and bank first.
3. **Protect your email above all** — it's the master key.
4. **Never sign in, pay, or share a code through a link someone sent you** — go to the site yourself.
5. **Never share a password or verification code** with anyone who contacts you.
6. **When pressured or unsure, slow down** and check with someone you trust.

Quick reference

Thing	What to do
Strong password	Long passphrase of random words; unique to one account.
Password manager	Apple Passwords, Google Password Manager, or a trusted standalone.
Turn on 2-step	Account → Settings → Security → Two-Step Verification.
Best second step	Passkey, then authenticator app, then text code (any beats none).
Backup codes	Save them when turning on 2-step — your spare key.
Phishing rule	Don't click links to sign in/pay — go to the site yourself.
Suspicious call	Hang up; call back using the number on your card. Don't trust caller ID.
Lost/stolen phone	Use Find My (Apple) or Find My Device (Google) to lock it.

Never, under any circumstances

- Give your password or a verification code to anyone who calls, texts, or emails you.
- Let a stranger connect to or "fix" your computer from a surprise contact.
- Move your money to a "safe account" because someone told you to.
- Pay with gift cards for "support," "fees," or "fines" — always a scam.

Keep handy	Fill in
My password manager	_____
My email has 2-step on	Yes / No (make it Yes!)
Bill's Home Tech	(330) 200-8042 · billshometech.com/book

FROM BILL

You're a hard target now

You've learned the habits that protect against the great majority of online trouble — and that's genuinely most of the battle. Use a manager, turn on two-step verification, guard your email, never share codes, and slow down when pressured. Do those, and you can enjoy your life online with confidence. I'm one phone call away for the rest. — Bill, (330) 200-8042