BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS · NO. 10

Staying Safe Online

Scams, passwords, privacy and peace of mind — explained in plain English, one step at a time

A calm, plain-English guide to protecting yourself

You don't need to be afraid — just unhurried

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

For phones, tablets and computers · facts current November 2026

What's Inside

This is your safety manual. Read it in any order and at your own pace — there is no test, and you can't fall behind. Keep it nearby and reach for whatever you need. My aim is not to frighten you. It's the opposite: a little calm know-how makes you nearly scam-proof, and that lets you enjoy your phone, your computer, your email and your shopping without that nagging worry. Scammers change their costumes constantly, so I won't just list tricks — I'll show you the *pattern* underneath them all, so you can spot a brand-new scam you've never seen before. Slow down, and you've already won.

Part 1 — The Master Key: How Scammers Think

1 A Note from Bill
2 The One Pattern Underneath Every Scam
3 The Three Feelings Scammers Reach For
4 The One Rule That Stops Nearly Every Scam
5 Things No Honest Person Will Ever Ask
6 How Scammers Reach You
7 Why You — and Why There's No Shame in It

Part 2 — The Scammer's Playbook

8 The Grandparent & Family-Emergency Scam
9 The Tech-Support Scam
10 The Romance Scam
11 The IRS & Tax Scam
12 The Social Security Scam
13 Medicare & Health-Insurance Scams
14 Prize, Lottery & Sweepstakes Scams
15 Investment & Cryptocurrency Scams
16 Phishing: Fake Emails That Fish for You
17 Smishing: Scam Text Messages
18 Zelle, Venmo & Bank-Impersonation Scams
19 QR-Code Scams
20 Charity, Disaster & "Good Cause" Scams
21 Online Shopping & Fake-Store Scams
22 Utility, Debt & "You Owe Money" Scams
23 The Refund & Subscription-Renewal Scam
24 Job, "Mystery Shopper" & Fake-Check Scams
25 Rental, Real-Estate & Vacation Scams
26 A Field Guide: Spotting Any Scam at a Glance

Part 3 — Passwords & Logins Done Right

27 Why Passwords Matter More Than You Think
28 What Actually Makes a Password Strong
29 The Password Manager: A Safe That Remembers For You
30 Using a Password Manager, Step by Step
31 Prefer Paper? The Password Book Done Safely
32 Two-Factor: The Deadbolt on Your Accounts
33 Turning On Two-Factor, Step by Step
34 Passkeys, Face ID & Fingerprint Login
35 Recovery, Security Questions & Keeping the Keys

Part 4 — Your Devices, Kept Safe

36 Your Devices Are Safer Than You Fear
37 The Single Best Habit: Keep It Updated
38 The Lock Screen: Your Device's Front Door
39 Antivirus: Myths, Truths & What You Actually Need
40 Scary Pop-Ups & Suspicious Downloads
41 Public Wi-Fi: Coffee-Shop & Airport Safety
42 Your Home Wi-Fi & Internet Box
43 Backing Up: So Nothing Is Ever Truly Lost
44 Spam Calls, Robocalls & Voicemail
45 Smart-Home Gadgets: Cameras, Doorbells & Speakers
46 Passing On a Device Safely: Wipe It First

Part 5 — Safe on the Web

47 The Padlock & "https": What "Secure" Means
48 Reading a Web Address Like a Pro
49 Reaching a Website the Safe Way
50 Spotting a Fake or Lookalike Website
51 The "Support Number" Trap in Search Results
52 Safe Online Shopping, Start to Finish
53 Safe Online Banking
54 Email Safety: A Closer Look
55 Links & Attachments: Look Before You Leap
56 Your Browser Is on Your Side
57 Cookies, Ads & Those "Accept" Boxes
58 Safe Video Calls With Family
59 When a Site Asks to Install, Allow, or Notify

Part 6 — Your Private Information

60 Why Your Information Is Worth Protecting

61 What's Safe to Share, and What Isn't
62 Oversharing on Social Media
63 Data Brokers & Why the Scam Calls Come
64 Shrinking Your Footprint
65 Handling Any Caller With Confidence
66 Guarding Your Most Sensitive Numbers
67 Freezing Your Credit: The Strongest Lock
68 Keeping an Eye on Things
69 Family, Caregivers & Shared Devices

Part 7 — If It Happens to You

70 First, Breathe — You're Going to Be Okay
71 The First Hour: Stop the Bleeding
72 If You Sent Money
73 If You Gave a Password or Code
74 If You Let Someone Into Your Computer
75 If Your Identity May Be Stolen
76 Where to Report It
77 Beware the Recovery Scam
78 Recovering Your Peace of Mind

Part 8 — Safe Habits & When to Call Bill

79 Building Safe Habits That Stick
80 Your Safety Checklist, Now and Then
81 Talking With Family About Scams
82 If You Think a Loved One Is Being Scammed
83 Staying Calm as the Scams Change
84 A Plain-English Safety Glossary
85 Your One-Page Scam Cheat-Sheet
86 When to Call Bill

PART 1

The Master Key: How Scammers Think

Before any list of tricks, I'll hand you the one idea that sits underneath all of them. Learn the pattern and you'll spot a brand-new scam you've never seen before. Calm, clear, and no fear-mongering.

CHAPTER 1

A Note from Bill

Hello, and welcome. Whoever is holding this book right now — this is for **you**. Maybe you've had a strange phone call or a text that didn't sit right, and you want to feel surer. Maybe a friend got caught by something and it shook you. Or maybe you simply want to use your phone, your computer, and the internet without that little knot of worry in your stomach. Wherever you're starting from, you've come to the right place, and I'm glad you're here.

I'm Bill. Helping folks feel at home and safe with their technology is what I do every day, and I wrote this book the same way I'd sit down next to you at your kitchen table: patiently, in plain English, with no rushing and no scary jargon. If I ever use a word you don't know, I'll stop and explain it right then — you won't have to look anything up.

My promise: this book will calm you down, not scare you

There's a lot of frightening talk out there about scams and hackers, and some of it is designed to sell you something. That's not what this is. My honest belief, after decades of doing this, is that fear is the *scammer's* tool, not mine. Frightened people make mistakes; calm people don't. So the whole purpose of this book is to replace that vague worry with a few clear habits — and once you have them, you can relax and enjoy everything the internet is good for.

WHAT THIS DOES FOR YOU

What you'll get out of this

By the end of this book you'll be able to spot the warning signs behind almost any scam — even one you've never seen — pick passwords that actually protect you, keep your devices tidy and safe, shop and bank online with confidence, and know exactly what to do if something ever does go wrong. Not from fear. From calm, quiet know-how.

The single most important sentence in this book

If you remember nothing else, remember this. **Scams only work when you're rushed. The moment you slow down and check with a real person, the spell breaks.** That's it. Everything else in these pages is just helping you build the habit of slowing down. You don't need to be clever or technical. You need to be unhurried — and you already know how to be that.

This book is yours — read it any way you like

You do not have to read these pages in order, and there's no test at the end. Start on page one, or flip straight to the chapter that answers today's question. Fold the corners, underline things, scribble in the margins. Keep it in the drawer by your chair and pull it out whenever something feels off. It's a reference, not a race — you cannot fall behind.

And I'm only a phone call away

This book will carry you a long way on your own. But if you ever get a message that worries you, or you just want a second opinion before you do anything, you are never stuck alone. Call me at **(330) 200-8042** and we'll work it out together, with no judgment and no eye-rolling. Asking me first is always the right move — it is never a bother, and it has saved a great many people a great deal of grief.

— Bill

CHAPTER 2

The One Pattern Underneath Every Scam

Let me hand you the master key straight away. There are hundreds of different scams, and new ones appear every month, but nearly every single one — no matter how it's dressed up — works the same way underneath. Once you can feel that pattern, you'll spot trouble a mile off, and you won't need to memorize a hundred separate tricks.

Every scam is the same three-step dance

Strip away the costume — the fake police officer, the sweetheart, the computer pop-up, the prize — and underneath, a scam almost always does these three things, in this order:

1. **It grabs your emotions.** It makes you suddenly afraid, excited, flustered, or sorry for someone. Strong feeling is the point, because feeling crowds out thinking.
2. **It rushes you.** "Act now." "Today only." "Before it's too late." The hurry exists so you won't stop, step back, and check.
3. **It asks you to *move* something** — money, a code, a password, remote access to your computer, or personal details — in a way that can't easily be undone.

That's the whole machine. Grab, rush, extract. When you learn to notice those three moving parts, the specific costume stops mattering. A "grandson in jail" and a "Microsoft virus warning" look nothing alike on the surface — but underneath, they're running the exact same play.

> **FROM BILL**
>
> **This is why I teach the pattern, not a list**
>
> A list of scams goes out of date the week it's printed, because the crooks keep inventing new costumes. The *pattern* never goes out of date. If you train your eye on "strong feeling + hurry + send something," you'll catch scams I've never even heard of yet. That's worth more than any list.

The good news hidden in the pattern

Here's the comforting part. Because every scam needs you to act *fast* and *alone*, every scam has the same simple weakness: **time** and **a second opinion**. You don't have to out-smart a professional crook. You just have to refuse to be hurried, and talk to one trusted person first. That tiny pause defeats the whole machine, because the machine only runs at speed.

WHAT THIS DOES FOR YOU

You already have the only tool you need

You don't need special software or technical skill to beat the pattern. You need a pause and a phone call. Both are free, and you already own them. Everything else in this book just makes that pause easier and more automatic.

CHAPTER 3

The Three Feelings Scammers Reach For

We said a scam starts by grabbing your emotions. Let's name the exact three feelings crooks reach for, because once you can feel one of these come over you, a little alarm bell should ring: *someone may be working me right now — time to slow down.*

1. Fear

"There's a warrant for your arrest." "Your Social Security number has been suspended." "Your computer is infected." "Your grandson is in jail." Fear is the scammer's favorite because it makes good, sensible people do things they'd never normally do. A frightened person stops thinking and starts obeying — which is precisely the plan.

2. Urgency

"Act now or your account will be closed." "You have two hours to pay." "Don't hang up." Urgency is fear's partner. It exists for one reason: to stop you from putting the phone down and checking with someone. Real companies and real government offices do not threaten you into hurrying. They send letters. They let you call back. They are patient — because they're real.

3. Something for nothing

A prize you didn't enter for, an inheritance from a stranger, a sweetheart who adores you within days, an investment that "can't lose." This one works on hope instead of fear, but it's the same trick. If an offer seems too good to be true, it is — every single time. Nobody gives money away to strangers, and no honest investment is ever guaranteed.

STAY SAFE

Feel the feeling, then slow down

You can't stop these feelings from happening — the crooks are skilled, and a good scam is genuinely upsetting or exciting in the moment. You don't have to. You just have to recognize the feeling as a *signal*: strong emotion plus pressure to act now is the fingerprint of a scam. When you feel it, that's your cue to stop, breathe, and check — not to act.

A quiet word about why this works on everyone

If you've ever thought "I'd never fall for that," I understand — but let me gently say that these scammers are full-time professionals who practice on thousands of people a day, and they

are very, very good at it. Doctors, lawyers, bankers, and yes, people far younger than us get caught. Being targeted says nothing about your intelligence. The only defense that works for *anyone* is the habit of slowing down — not cleverness. So let's build the habit.

CHAPTER 4

The One Rule That Stops Nearly Every Scam

If this book had to shrink to a single sentence and a single card you kept in your wallet, this chapter is what it would say. It is the most powerful thing in these pages, and it's wonderfully simple.

FROM BILL

Bill's one rule

Slow down, and never send money, codes, passwords, or remote access to your computer because of a message, a call, or a pop-up. No matter who it claims to be. No matter how urgent it sounds. Hang up or close it, take ten minutes, and check with a real person — your bank, your family, or me — using a number *you* look up. That one habit stops the overwhelming majority of scams cold.

Why this one rule is so powerful

Remember the pattern: every scam needs you to move something — money, a code, access — quickly and alone. This rule simply refuses to do that until you've paused and checked. It doesn't require you to figure out whether the call is real. You don't have to win an argument with a crook or spot a clever fake. You just decline to act in the moment. The crook's whole plan falls apart the instant you say, "I'll call you back," and hang up.

The magic words to keep ready

It helps to have a sentence rehearsed, so you're not caught flat-footed when someone pressures you. Any of these work beautifully, and you do not owe anyone an explanation:

- "I don't make decisions over the phone. I'll call back on a number I look up myself."
- "Thank you, I'm going to check with my family first. Goodbye."
- "No. I never send money or codes because of a call." — and then hang up.

You are allowed to hang up on anyone, even if they sound official, even mid-sentence. Hanging up on a scammer is not rude — it is exactly the right thing to do. A real organization will never mind you calling them back; a scammer will fight hard to keep you on the line. That fight is itself a dead giveaway.

TIP

"I'll call you back" is your superpower

Scammers cannot survive those four words. If anyone resists you hanging up and calling back — "Don't put the phone down," "Stay on the line," "There's no time" — that resistance is proof. Real callers are happy for you to verify. Only crooks need you to stay on the line right now.

CHAPTER 5

Things No Honest Person Will Ever Ask

Here's a short list you can almost treat as law. Certain requests are so reliably the mark of a scam that the moment you hear one, you can stop worrying about the details and simply say no. Honest people and real organizations never ask for these.

Payment by gift card

This is the big one, so let me say it as plainly as I can. **No real business, government office, utility, or tech company is ever paid with gift cards.** Not the IRS. Not Social Security. Not Medicare. Not Microsoft or Apple. Not your electric company. Not a bail bondsman. Gift cards — the ones you buy at the grocery store, like Apple, Amazon, Google Play, or Target cards — are the scammer's favorite because once you read them the numbers on the back, the money is gone forever and cannot be traced or refunded.

SCAM ALERT

Gift cards are the brightest red flag there is

Burn this into memory: **anyone — ever — who tells you to buy gift cards and read them the numbers over the phone is a scammer. 100% of the time. No exceptions.** There is no legitimate situation in the entire world where a real debt, fine, fee, or purchase is paid that way. If you remember only one fact from this book, make it this one.

A verification code sent to your phone

A "code" or "one-time passcode" texted to your phone is a key to *your* account. The whole point of it is that only you ever see it. **Never read a code aloud or type it into a box because someone asked you to.** A real company sends you that code so *you* can log in — they will never phone you and ask you to tell it back to them. Anyone asking for your code is trying to break into your account.

Your password, or remote control of your computer

No real bank, company, or support line will ever ask for your full password, and no honest caller will ask you to install a program that lets them "take a look" at your computer from far away. That remote-control trick is how crooks pretend to "fix" a problem while they actually empty your accounts. We'll cover it fully in Part 2 — for now, just know: nobody legitimate calls *you* and asks to drive your computer.

Secrecy

"Don't tell anyone." "Keep this between us." "Don't mention it to your family or the bank teller." Honest dealings are never secret. The instant someone asks you to hide what you're doing from the people who love you, you are being scammed. That request for secrecy exists for one reason: the people who love you would stop you.

STAY SAFE

Unusual payment methods are all red flags

Besides gift cards, be deeply suspicious of any demand to pay by wire transfer (Western Union or MoneyGram), by a money app like Zelle, Venmo, or Cash App to someone you don't know, by cryptocurrency ("Bitcoin"), or by mailing cash. Crooks love these because the money vanishes and can't be clawed back. Real companies take normal, reversible payments and send a real bill you can check.

CHAPTER 6

How Scammers Reach You

A scammer has to get a message to you somehow, and there are only so many doorways into your life. Knowing the doorways helps, because each one has a simple safety habit attached. Let's walk through them calmly.

The main doorways

How they reach you	What to know
Phone call	A live voice, often "spoofed" to show a fake, official-looking number. Highest losses per victim, because a person can pressure you in real time.
Text message	Called "smishing." A short text with a link or a demand — a fake delivery, a fake toll, a fake bank alert. Cheap for crooks to send by the million.
Email	Called "phishing." A message that looks official, with a link to a fake login page or an alarming attachment.
Pop-up on screen	A sudden scary window — "Your computer is infected, call this number" — while you're browsing. Almost always fake.
Social media	A friend request, a message, a too-good deal, or a cloned account of someone you know. A very common starting point now.
Postal mail	A letter about a prize, a sweepstakes, or a fake invoice. Older-fashioned, but still around.

The one habit that covers all of them

Here's the lovely thing: the safety habit is the same no matter which doorway a message comes through. **Don't act on the message itself.** Don't call the number *it* gives you. Don't click the link *it* provides. Instead, if you think it might be real, reach the company or person *yourself* — using a phone number from the back of your card, a statement, the phone book, or by typing their website address in yourself. Going your own way to the real place sidesteps every fake doorway at once.

GOOD TO KNOW

"Spoofing" — why the number looks real

Crooks can make your phone display any name or number they like — "IRS," "Social Security," even your own bank's real number. This is called spoofing, and it's easy for them to do. So the number showing on your phone proves *nothing*. That's exactly why the habit is to hang up and call back on a number you look up yourself, not the one that called.

TIP

A quiet phone is a safe phone

You are never obligated to answer a call from a number you don't recognize. Let it go to voicemail; if it's real and important, they'll leave a message and you can call back on your own terms. Simply not answering unknown calls removes a whole category of pressure from your day.

CHAPTER 7

Why You — and Why There's No Shame in It

Let's have an honest, gentle conversation about something that goes unspoken too often. Scammers do target older folks on purpose — but *why* they do is not what you might think, and understanding it takes away both the fear and the shame.

Why crooks target our generation

It isn't because older people are foolish — far from it. It's a cold business calculation. Our generation is more likely to have savings, a home, and good credit built up over a lifetime of hard work. We were also raised to be polite, to trust, to respect authority, and to not want to make a fuss — all lovely qualities that a crook twists against us. And many of us are home during the day to answer the phone. None of that is a flaw in you. It's a flaw in them.

Being targeted is not the same as being foolish

I want to be very clear, because this matters: **everyone** is targeted, and plenty of sharp, careful, educated people get caught — including young people who grew up with this technology. The scammers are organized, full-time professionals with scripts refined on thousands of victims. When someone falls for a scam, it is a measure of how skilled the criminal was, not of any failing in the victim.

> **FROM BILL**
>
> **If it has already happened to you**
>
> If you're reading this because something already went wrong, please hear me: you are not foolish, you are not alone, and there is nothing to be ashamed of. I have helped many good, smart people through exactly this, and not once have I thought less of them. Part 7 of this book walks you calmly through what to do. And my phone is always on: (330) 200-8042. No lecture, ever.

Silence is the scammer's best friend

Here's why shame is dangerous, not just unkind: when people are embarrassed, they stay quiet. They don't tell their family, they don't report it, and so the crook gets away clean and moves on to the next person. Talking about scams — openly, without blame — is how we protect each other. If something happens to you, telling someone isn't weakness. It's how the damage gets stopped and how the next person gets warned.

WHAT THIS DOES FOR YOU

Turning worry into quiet confidence

The goal of this whole book is to move you from "I'm nervous and I don't quite understand this" to "I know the pattern, I know my one rule, and I know who to call." That shift — from vague worry to calm, specific confidence — is the real protection. Let's keep building it.

PART 2

The Scammer's Playbook

A calm field guide to each major scam aimed at folks like us — one chapter each. You don't need to memorize them; you'll see the same pattern from Part 1 wearing a dozen costumes. That's the point.

CHAPTER 8

The Grandparent & Family-Emergency Scam

This one is cruel, because it weaponizes your love for your family. It's also one of the most common, so let's take it slowly and make you immune to it.

How it works

The phone rings. A frightened young voice says "Grandma? It's me." You say a name — "Michael?" — and now the crook knows what to call themselves. The story tumbles out: there's been an accident, or an arrest, they're hurt or in jail, they're mortified, and they need money *right now* — and please, **don't tell Mom and Dad.** Sometimes a second voice comes on as a "lawyer" or "police officer" to make it sound official. They'll want gift cards, a wire, cash in an envelope, or a money app.

The tells

- A **frantic, emotional** call that makes you afraid for a loved one.
- A plea for **secrecy** — "don't tell the family" — which no real emergency ever needs.
- A demand for **money fast**, by gift card, wire, cash, or app.
- Vagueness about details, and pressure to stay on the line and not check.

STAY SAFE

Hang up and call your family on the number you already have

This is the whole defense, and it never fails: **hang up, and call your grandchild (or their parents) directly on the number you already have saved.** You'll almost always find them safe at home, baffled. The crook is betting you won't check. Prove them wrong. Even if the voice sounds right — crooks can now fake voices — the call-back still catches it.

GOOD TO KNOW

A family code word works wonders

Many families now agree on a **secret word or question** that any real emergency call must include — something only the family would know, not posted anywhere online. If a caller claiming to be family can't give it, you know. Pick one at your next get-together; it costs nothing and gives great peace of mind.

CHAPTER 9

The Tech-Support Scam

If you use a computer, this is the scam most likely to come knocking. It's the one where "Microsoft" or "Apple" supposedly calls to warn you about a virus — and it's always fake.

The two ways it starts

- **A pop-up** suddenly fills your screen while you're browsing: flashing warnings, maybe an alarm sound, "YOUR COMPUTER IS INFECTED — Do not shut down — Call this number now."
- **A phone call** out of the blue from "Microsoft," "Apple," or "tech support" saying they've "detected a problem" with your computer.

Where it goes

Either way, they want you to call a number and then let them **connect to your computer** to "fix" it (using a remote-control program). Once in, they put on a show of "finding" problems, then charge you hundreds of dollars — often demanding gift cards — and sometimes quietly open your bank website while they're in there. The "virus" was never real. The only problem was the person on the phone.

SCAM ALERT

Real tech companies never call you about a virus

Here is the clean, simple truth: **Microsoft, Apple, Google, and your internet company will never phone you, and will never put a pop-up on your screen telling you to call a number.** They don't monitor your computer that way and they don't work like that. So any such call or pop-up is, with no exceptions, a scam. You can dismiss it entirely.

What to do

1. **Don't call the number.** Don't let anyone connect to your computer. Don't pay.
2. For a scary pop-up: close the window if you can, or simply **restart the computer** (turn it off and on). The pop-up is just a web page; restarting clears it.
3. For a call: hang up. You don't owe them a conversation.
4. If you did let someone in, or paid, turn to Part 7 — and call me. It's fixable, and we'll stay calm about it.

FROM BILL

If a pop-up ever traps you, just call me

A full-screen scary pop-up can feel like a hostage situation — the buttons won't work, there's a siren noise, it says don't shut down. Ignore all of that. It's a bluff. Hold the power button to turn the machine off, wait, turn it back on, and it's gone. Or call me at (330) 200-8042 and I'll talk you through it in two minutes. You did nothing wrong.

CHAPTER 10

The Romance Scam

Romance scams are among the cruelest, because they prey on kindness and loneliness, and they unfold slowly — over weeks or months — so the trap closes gently. Knowing the pattern is your best protection, and there's no shame in any of it.

The pattern

- A charming stranger appears — through a dating site, a social-media message, or even a "wrong number" text that turns friendly — often claiming to work far away (an oil rig, the military overseas, a doctor abroad, a contractor on a big job).
- They're warm and attentive **quickly**, and talk of strong feelings sooner than feels ordinary. This is called "love bombing."
- They always have a reason they **can't meet in person or video-call** clearly.
- Eventually a crisis arrives — a medical bill, a frozen account, a customs fee, a plane ticket home — and a request for money. Then another. And another.

STAY SAFE

If you've never met them in person, never send money

A simple, protective rule: **no one you've only met online or by phone should ever receive money, gift cards, or crypto from you** — no matter how real the feelings are, no matter the emergency. A genuine person will understand and will never pressure you. Pressure for money is itself the proof it's a scam.

The investment twist

A very common modern version mixes romance with investing. The sweetheart isn't short of money — instead they want to *share their good fortune*, teaching you to "invest" in crypto through a special app or website. The profits look wonderful on the screen. They are not real, and when you try to withdraw, the fees and taxes never end. We cover this in its own chapter — just know the romance and the "opportunity" are the same crook.

FROM BILL

There's no shame here, and it's never too late to stop

These scammers are professionals who run this play on many people at once; being targeted says nothing bad about you, and plenty of sharp, warm-hearted people have been fooled. If you ever worry you're caught up in one, the kindest thing you can do is talk to someone you trust — family, or me. No judgment. We just help you stop and get you safe.

CHAPTER 11

The IRS & Tax Scam

"This is the IRS. You owe back taxes, and there's a warrant for your arrest unless you pay today." It's a frightening call by design. It is also, every single time, a scam.

How the real IRS actually works

Knowing how the genuine IRS behaves makes the fakes obvious. The real IRS:

- **Contacts you first by mail**, through the U.S. Postal Service — not by a surprise phone call, text, or email.
- **Never demands immediate payment** by phone, and always gives you the chance to question or appeal what you owe.
- **Never asks for gift cards, wire transfers, or cryptocurrency**, and never asks for your card number over the phone.
- **Never threatens to send police** to arrest you over a tax bill.

SCAM ALERT

"Warrant for your arrest" means it's fake

Any caller who threatens you with immediate arrest, deportation, or jail over taxes is a crook. The IRS simply does not operate that way. Hang up. If you're genuinely unsure whether you owe anything, don't use any number the caller gave you — look up the IRS yourself at irs.gov or on a letter they've actually mailed you.

Tax-season variations

Around tax time, watch also for fake "tax preparers" who promise huge refunds and then disappear with your information, and for emails pretending to be from the IRS with a link to "claim your refund." The IRS doesn't email you links to claim refunds. When in doubt, go to irs.gov yourself, or ask a tax professional you found independently.

CHAPTER 12

The Social Security Scam

A close cousin of the IRS scam, this one claims to come from the Social Security Administration — and it frightens people because Social Security is a lifeline.

The usual story

A call or recorded message says your **Social Security number has been "suspended"** because of "suspicious activity" or a crime linked to your name, and you must "confirm" your number or pay a fee to fix it. Sometimes they say your benefits will stop unless you act. All of it is false.

GOOD TO KNOW

Your Social Security number can't be "suspended"

Here's a fact that defeats this scam instantly: **a Social Security number is never suspended, cancelled, or frozen.** There's no such thing. The real Social Security Administration will not call to threaten you, won't demand payment by gift card or wire, and won't ask you to "confirm" your number out of the blue. Any call that does is a scam.

What to do

- Hang up on any threatening or robotic call about Social Security.
- Never read your Social Security number aloud to someone who called *you*.
- If you want to check your real account, go to **ssa.gov** yourself or call Social Security using the number on their official website or your own paperwork — never a number a caller gives you.

TIP

Guard those nine digits

Your Social Security number is one of the most valuable things a crook can get, because it helps them open accounts in your name. Don't carry the card in your wallet, don't say the number aloud where others can hear, and never give it to someone who contacted you first. When a form asks for it, it's fair to ask whether they truly need it.

CHAPTER 13

Medicare & Health-Insurance Scams

Around open-enrollment time especially, the phone fills up with calls about Medicare. Some are pushy salespeople; some are outright crooks. Here's how to stay calm and in control.

What they're after

Most Medicare scams want one of two things: your **Medicare number** (which they can use to bill for fake services, called "Medicare fraud") or to sign you up for a plan you don't want so they earn a commission. The hooks include a "new card" (there's a chip in it now!), "free" braces, test kits, or equipment, or a warning that your coverage will lapse unless you "verify" your details.

SCAM ALERT

Medicare won't call you out of the blue for your number

Medicare does not call you uninvited to ask for your Medicare number or bank details, and there is no new card you must pay or "verify" to receive. Treat your Medicare number like a credit card number — give it only to doctors and providers *you* chose and contacted. Anyone phoning you for it is up to no good.

Staying safe and checking the real thing

- Don't accept "free" medical equipment, genetic tests, or braces offered by phone — these are classic fraud setups.
- Read the statements Medicare sends and watch for services or items you never received; report anything odd.
- For anything genuine, use the official line — **1-800-MEDICARE** (1-800-633-4227) — or **medicare.gov**, which you reach by typing it in yourself.

FROM BILL

I'm not here to sell you a plan

A gentle word: I help you stay *safe*, I don't sell insurance, and I'd be wary of anyone who mixes the two. If you want help comparing real Medicare options, your State Health Insurance Assistance Program (SHIP) offers free, unbiased counseling. I'm glad to help you find it — just call me.

CHAPTER 14

Prize, Lottery & Sweepstakes Scams

"Congratulations — you've won!" It's a lovely thing to hear, which is exactly why crooks use it. The catch is always the same, and once you see it, you'll never be caught.

The unmissable catch

Whether it's a lottery, a sweepstakes, a "second-chance" drawing, or a prize from a lookalike company, the trap is always a **payment you must make first**: a "fee," a "tax," "insurance," "customs," or "shipping" to release your winnings. Or they ask for your bank details "to deposit the prize." Either way, you lose.

STAY SAFE

Two facts that end every prize scam

One: you cannot win a contest you never entered. Two: a real prize never requires you to pay anything to receive it. Legitimate winnings don't come with upfront fees or taxes you pay to the sender. The moment someone asks you to pay to collect, it's a scam — stop there.

Famous-name versions

Crooks love to borrow trusted names — a well-known sweepstakes company, a big retailer, even a lottery from another country. They may send official-looking letters or a fake check (which bounces after you've spent it). Don't deposit surprise checks, don't pay fees, and don't give bank details to collect a prize. When in doubt, throw it out.

CHAPTER 15

Investment & Cryptocurrency Scams

This is now the scam that steals the *most money* from older adults, so it deserves a careful, calm look. These schemes promise to grow your savings fast, and they can be slick and very convincing. The warning signs, happily, never change.

What they look like

- Promises of **big, guaranteed returns** with "no risk" or "can't lose." Real investing never guarantees big returns; anyone who says so is lying.
- A friendly "mentor," a new online friend, or a sweetheart who shows you screenshots of their profits and offers to help you do the same.
- Pressure to invest through a **particular app or website** you were steered to, often using **cryptocurrency** ("Bitcoin").
- A dashboard that shows your money growing beautifully — then endless "fees" and "taxes" whenever you try to withdraw.

STAY SAFE

If you can't get your money back out, it was never there

This is the cruel signature of these scams: your "account" shows lovely profits, but every time you try to withdraw, there's one more fee, one more tax, one more delay. The money was gone the moment you sent it. Before you invest a cent in anything you heard about online or from a new contact, talk to a *licensed* financial professional you found independently — and talk to your family.

"Pig butchering" — the long con

You may hear this ugly nickname for the slow version: a scammer spends weeks building trust and friendship (or romance) before ever mentioning money, then introduces the "investment." The relationship is fake from day one. The length of it is a feature, not a reassurance — the longer they invest in you, the bigger the theft they're planning.

FROM BILL

Run it past someone before you send a dime

I'm not a financial advisor and I won't pretend to be. But I'll tell you this: every "amazing opportunity" that arrives through a message, an online friend, or a sweetheart deserves a hard pause and a conversation with people who love you before any money moves. That one habit — talk first, never send in a hurry — protects more folks than anything else I know.

CHAPTER 16

Phishing: Fake Emails That Fish for You

"Phishing" (said "fishing," and that's exactly what it is) is when a crook dangles a bait email hoping you'll click a link and hand over a password or card number. It's behind a huge share of stolen accounts — and once you see how it works, you'll dodge it every time.

How the trick works

You get an email that looks official — from "your bank," "Amazon," "Netflix," "Apple," the post office, even "Microsoft." It says there's a problem: a suspicious charge, an account on hold, a password expiring, a payment that failed. There's a **button or link** to "fix" it. The link leads to a page that looks exactly like the real login — but it's a counterfeit, and the moment you type your password there, the crook has it.

How to beat it, every time

- **Never log in through a link in an email.** Open the company the way you always do — your own app, or by typing the address yourself (amazon.com, your bank's address).
- **Distrust urgency.** "Act within 24 hours or your account closes" is the sound of a scam, not of a real company.
- **Look, don't leap.** Odd sender addresses, a greeting that isn't your name ("Dear Customer"), spelling mistakes, and slightly-wrong web addresses are all tells — but the first rule alone keeps you safe even when the fake is flawless.
- **Never open an unexpected attachment**, especially a file you weren't expecting. It can carry a virus.

SCAM ALERT

The "failed payment" and "your order" classics

Two of the most common lures: "Your payment didn't go through — update your card" and "Your order for $499 has shipped — click here if this wasn't you." Both aim to panic you into clicking. Don't. If you're worried, open your real account directly and check. The fake order never existed; your real account will show no such charge.

CHAPTER 17

Smishing: Scam Text Messages

"Smishing" is just phishing by text message. Texts feel personal and urgent, and they're dirt cheap for crooks to blast out by the million — so you'll see plenty. Here are the ones going around, and the single habit that beats them all.

The texts you'll see

The text	What it really is
Fake package delivery	"USPS/UPS/FedEx: your package is held — confirm your address/pay a small fee" with a link. The post office does NOT text you asking for details or payment.
Fake unpaid toll	"You have an unpaid toll of $6.99 — pay now to avoid a late fee" claiming to be E-ZPass or your state's toll road. A very common 2025 wave.
Fake bank alert	"Did you make a $750 purchase? Reply NO" — then a "fraud agent" calls to "help" you move your money (into their hands).
"Wrong number" chit-chat	A friendly stranger texts as if they misdialed, then keeps chatting — the opening move of a romance or investment scam.
Fake account/code	"Your account is locked — verify here," or a text asking you to forward a code you just received.

STAY SAFE

Don't tap links in texts — go to the source yourself

The one habit that beats every scam text: **don't tap the link.** If you think a delivery, toll, or bank message might be real, check it *yourself* — open the delivery company's own app or tracking page, log in to your toll account the way you normally do, or call your bank on the number from the back of your card. Never through the text's link.

What to do with a scam text

1. **Don't tap** any link and don't reply (even "STOP" tells them a real person is there).
2. **Delete it.** You can also report it: forward scam texts to **7726** (it spells "SPAM"), a free service your phone company runs.
3. If it pretends to be a company you use, and you're worried, contact that company directly to be sure — never through the text.

GOOD TO KNOW

Real delivery and toll alerts look different

Genuine shipping updates come through the delivery company's own app or the tracking number you got when you ordered, and they never ask for a payment or your card by text. Real toll agencies bill you by mail or through the account you set up. If a text is pushing you to pay or "confirm" right now via a link, that urgency is the scam.

CHAPTER 18

Zelle, Venmo & Bank-Impersonation Scams

Money apps like **Zelle**, **Venmo**, and **Cash App** move money between people instantly — which is handy with family, and dangerous with strangers, because once it's sent, it's almost always gone for good. Crooks have built a whole scam around this.

The "fraud department" trick

It usually starts with a text or call: "Did you just send $500 on Zelle? Reply NO if not." You reply NO (or call the number), and a calm "fraud agent" from "your bank" walks you through "reversing" or "protecting" the payment — which actually means sending your own money straight to *them*, often by telling you to "send it to yourself." There's no reversal. You're being guided to rob yourself.

SCAM ALERT

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

Burn this in: **no real bank ever tells you to move your money to another account, send it to yourself, or send it anywhere "to protect it" from fraud.** That instruction, from anyone, is always the scam itself. If a "bank" caller says it, hang up and call your bank on the number from the back of your card.

Treat these apps like cash

- Only send money through these apps to people you **personally know and trust**. Treat it like handing over cash — there's usually no getting it back.
- Never use them to "pay" a company, a fee, a deposit, or a stranger from an ad or a call.
- Double-check you've got the right person before sending; the money goes instantly.
- Ignore "accidental payment, please send it back" messages — the original was faked and will vanish, leaving you out the amount you "returned."

CHAPTER 19

QR-Code Scams

A **QR code** is that little square of black-and-white dots you point your phone's camera at to open a website — handy for menus and parking. Crooks have learned to use them too, so a quick word of care goes a long way.

How the trick works

Because a QR code is just a hidden web address, you can't read it with your eyes — you only find out where it goes after you've scanned it. Scammers exploit that: they stick fake codes over real ones on parking meters and signs, mail official-looking letters with a code to "pay a fine," or put codes in scam emails and flyers. The code sends you to a fake page that steals your card details or password.

STAY SAFE

Look before you leap — check the address the code opens

When you scan a QR code, your phone shows the web address before it opens. **Pause and read it.** If it's not the plain, expected website (your city's real parking site, say), don't continue. Be especially wary of codes on stickers, in unexpected mail, or in emails — and never scan a code to "pay a fine" or "claim" something.

Safer habits

- Prefer typing a known web address yourself over scanning a code, especially for anything involving payment.
- At a parking meter or kiosk, check the code sticker isn't pasted over another one.
- Treat a QR code in an unexpected letter, email, or text exactly like a suspicious link — because that's what it is.

CHAPTER 20

Charity, Disaster & "Good Cause" Scams

Your generosity is a wonderful thing — and crooks try to exploit it, especially after a hurricane, wildfire, or other disaster is in the news, or around the holidays. A little care lets you give safely and still give freely.

The warning signs

- Pressure to give **right now**, and gratitude that turns pushy if you hesitate.
- A charity name that sounds *almost* like a famous one, but a touch off.
- A request to pay by **gift card, wire, cash, or money app** — real charities don't ask for those.
- A caller who thanks you for a "pledge" you don't remember making, to jog a false memory.

TIP

Give on your own terms, to a charity you chose

The safe habit: don't give in response to a surprise call, email, or door-knock. Instead, decide which causes you want to support, and give by going to that charity's real website or mailing a check *yourself*. You can check any charity for free at a watchdog site like Charity Navigator or the BBB's Give.org before you give a cent.

CHAPTER 21

Online Shopping & Fake-Store Scams

Most online shopping is safe and genuinely wonderful — things delivered to your door, often cheaper. But a few bad actors set up fake shops and too-good deals, so here's how to tell the good from the bad. (Part 5 covers safe shopping in full; this is the scam side.)

Signs of a fake or rip-off store

- Prices that are **wildly** below everyone else — the classic bait.
- A brand-new website you've never heard of, reached through a social-media ad, with no real company address or phone number.
- Only odd payment options — wire, gift card, crypto, or a money app — and no normal credit card checkout.
- Pressure timers, "only 2 left!", and reviews that all sound the same.
- Goods that never arrive, or cheap knock-offs instead of what you ordered.

STAY SAFE

Pay by credit card for the protection

When you shop online, **a credit card is your safest friend**, because if something goes wrong you can dispute the charge and get your money back. Debit cards, money apps, wires, and gift cards offer little or no such protection. If a store won't take a normal credit card, that's a reason to shop elsewhere.

GOOD TO KNOW

Check before you buy from a new shop

Before buying from a store you don't know, do a quick search for its name plus the word "scam" or "reviews," and look for a real address and contact details on the site. A minute of checking saves a lot of bother. When a deal feels too good to be true, it usually is.

CHAPTER 22

Utility, Debt & "You Owe Money" Scams

A whole family of scams works by claiming you owe money and must pay instantly or face disaster. The costume changes — the power company, a court, a debt collector — but the pattern is the one you already know.

The usual threats

- **Utility shut-off:** "Your electricity will be cut off in one hour unless you pay now." Often aimed at businesses, but at homes too.
- **Fake debt collector:** a caller demanding payment on a debt you don't recognize, with threats of court or arrest.
- **"Jury duty" or "warrant":** a "sheriff" says you missed jury duty and must pay a fine by gift card to avoid arrest. Courts never do this.

SCAM ALERT

No real utility or court takes gift cards — or threatens instant arrest

Your power company will never demand a gift-card payment within the hour, and no court or police force collects fines by phone or threatens to arrest you over a missed payment. These are scams wearing a uniform. Hang up, and if you're worried about a real bill, call the utility on the number printed on your actual statement.

What to do

1. Don't pay anything in the moment, and don't be rushed by threats.
2. Hang up and verify independently: call your utility, court, or creditor using a number from your own bill or their official website.
3. Remember your rights: real debt collectors must, if you ask, send you written proof of a debt — they can't just demand instant payment by gift card.

CHAPTER 23

The Refund & Subscription-Renewal Scam

This one has become enormously common, and it's clever because it arrives looking like a routine receipt rather than a threat. It usually wears the name of an antivirus or tech company — "Norton," "McAfee," "Geek Squad," "PayPal."

How it works

You get an **email that looks like an invoice**: "Your subscription has auto-renewed for $399.99. If you didn't authorize this, call this number to cancel and get a refund." You never signed up for anything, so you call — and that's the trap. The "agent" offers a refund, has you log in to your bank or install a remote-control program, then pretends to "accidentally" refund too much and begs you to send back the difference (often in gift cards). The overpayment was faked; the money you send back is real.

SCAM ALERT

A surprise "invoice" is bait to make you call

The whole purpose of that scary renewal charge is to get *you* to call *them* — so it feels like your idea, which lowers your guard. **Don't call the number in the email.** You weren't charged; there's nothing to cancel. If you're genuinely unsure, check your real bank or card statement yourself (your own way), and you'll see no such charge.

What to do

- Don't call the number, don't reply, and don't click anything in the email — just delete it.
- If you truly want to check a subscription, go to that company or your card account your own way, never through the email.
- Remember: no honest refund ever requires you to install software, log into your bank on a call, or send money *back* by gift card.

CHAPTER 24

Job, "Mystery Shopper" & Fake-Check Scams

Scams dressed up as easy money or a friendly job offer are on the rise — and many hinge on a fake check, which is worth understanding once so it never catches you.

The fake-check trick at the heart of it

In many of these, you're sent a **check** and asked to deposit it, keep a portion as your "pay," and send the rest on — to "buy gift cards to evaluate," "cover fees," or "pay a vendor." Here's the catch that defines the scam: your bank may let you spend the money before the check is found to be **fake**, days later. When it bounces, the bank takes back the full amount — and the money you already sent on is gone, out of your own pocket.

The costumes it wears

- A **work-from-home job** or "reshipping" role that pays you to forward packages or money.
- A **mystery-shopper** gig that has you "evaluate" a store by buying gift cards.
- An **overpayment** for something you sold online, with a request to refund the extra.
- A **grant, prize, or legal settlement** that sends a check but asks for fees first.

STAY SAFE

Never send money back from a check you deposited

A simple rule defeats every version: **if anyone sends you a check and asks you to send part of it back or buy gift cards with it, it's a scam.** Real employers don't pay you before you work, and real prizes don't arrive by check with fees attached. When money flows *out* of a deal that was supposed to pay *you*, stop.

CHAPTER 25

Rental, Real-Estate & Vacation Scams

Looking for a place to rent, a vacation home, or helping a grandchild find an apartment? Crooks post listings for homes they don't own, to pocket your deposit. A little care keeps the search safe.

How it works

A crook copies photos and details of a real home (sometimes a real for-sale listing) and advertises it for rent or a cheap vacation stay. When you're interested, they spin a reason they can't show it in person — they're "out of the country," a "missionary," moved for work — and ask for a **deposit or first month's rent up front** by wire, gift card, or money app to "hold" it. You send it; there's no home, and they vanish.

Staying safe

- **See it in person** (or have someone you trust see it) before paying anything.
- Be suspicious of prices well below the local norm and of any landlord who won't meet or show the property.
- Never pay a deposit by **wire, gift card, or money app** to someone you haven't met and verified.
- Search the listing's photos and address online — if the same home appears elsewhere under a different name or for sale, it's a scam.

HEADS UP

"I'm away, just send the deposit" is the tell

The thread running through every rental scam is a landlord who can't meet you in person yet wants money up front in an untraceable way. A real landlord or agent will let you see the place and pay by normal means. When you can't see it and they're rushing your deposit, walk away.

CHAPTER 26

A Field Guide: Spotting Any Scam at a Glance

Let's gather the whole playbook into one quick-reference table you can keep by the chair or the phone. When something arrives and you're not sure, run down this list. If you spot the warning sign, you already know what to do: **slow down, don't send anything, and check with someone using a number you look up yourself.**

If you hear or see…	What it almost certainly is
"Buy gift cards and read me the numbers"	A scam — always, no exceptions
"Your SSN is suspended" / "warrant for arrest"	A government-impersonation scam
"Microsoft/Apple" warning you of a virus	A tech-support scam — hang up / restart
A frantic "grandchild" needing secret cash	A family-emergency scam — call them back
"You've won!" but must pay a fee first	A prize scam — you can't win what you didn't enter
"Guaranteed" big investment returns, no risk	An investment/crypto scam — talk to family first
"Did you make this charge? Reply NO" + call	A bank-impersonation / Zelle scam
A text link for a package, toll, or account	Smishing — go to the source yourself, don't tap
An online sweetheart who needs money	A romance scam — never send money
"Move your money to keep it safe"	Always the scam itself — your bank never says this
"Don't tell anyone" / "stay on the line"	A scam — secrecy and urgency are the fingerprints

WHAT THIS DOES FOR YOU

You now know the whole playbook

If you've read this part, you're better prepared for scams than a great many people half our age. You don't need to fear the phone or the computer — you need to be *unhurried*, and now you are. Everything from here on simply strengthens your defenses: good passwords, tidy devices, safe browsing, and knowing what to do if something slips through.

PART 3

Passwords & Logins Done Right

Passwords feel like a chore, but a few simple ideas make them both stronger and easier. We'll take the worry out of them — including the tools that remember them for you — so you never have to juggle a hundred in your head.

CHAPTER 27

Why Passwords Matter More Than You Think

Your password is the key to your digital front door — your email, your bank, your photos. And here's a truth worth knowing: your **email password** is the master key to almost everything else, because that's where "reset my password" messages for all your other accounts arrive. Protect your email, and you've protected a great deal at once.

The one mistake nearly everyone makes

If I could fix a single habit for everyone, it would be this: **don't use the same password in more than one place.** Here's why it matters so much. From time to time, a company gets "hacked" and a list of its customers' passwords is stolen — this happens through no fault of yours. Crooks then take that password and try it on your email, your bank, everywhere. If you've reused it, they're straight in. If each account has its own password, one break stays contained to that one place.

STAY SAFE

Different password for every account — especially these

At the very least, make sure your **email**, your **bank**, and your main **shopping** accounts each have their *own* unique password that you use nowhere else. If juggling that sounds impossible — it isn't, and this part shows you two easy ways (a password manager, or a simple paper book). You won't have to memorize them all.

What a stolen password really risks

This isn't about fear — it's about knowing what you're protecting, so the effort makes sense. A crook with your email password can read your messages, see which bank you use, reset your other passwords, and lock you out. A unique, strong email password plus the "deadbolt" we'll add later (two-factor) makes that nearly impossible. A little care here protects everything downstream.

CHAPTER 28

What Actually Makes a Password Strong

For years we were all told to make passwords with a jumble of capitals, numbers, and symbols — things like "P@ssw0rd!" that are impossible to remember and, it turns out, not even very strong. The experts have since changed their advice, and the new advice is wonderful news for all of us.

Length beats complexity

The single most important thing about a password is how **long** it is — not how many odd symbols it has. A long password made of ordinary words is far harder for a crook's computer to crack than a short jumble, and far easier for *you* to remember. The official guidance now favors long, memorable phrases over short, cryptic ones. Aim for something genuinely long — think a dozen characters or more.

GOOD TO KNOW

Why length wins

Crooks guess passwords with computers that try millions of combinations. Each extra character makes their job dramatically harder — adding length is like adding more and more locks. A four-word phrase can be stronger than a short scramble of symbols, and you'll actually remember it. Long and memorable beats short and clever.

The three-random-words trick

Here's a method anyone can use to make a strong, memorable password: **string together three or four random, unrelated words**, and sprinkle in a number or capital if a site insists. The words should be random — not a famous phrase. For example (don't use these exact ones): **CopperTurtleWindow**, or **brave-lemon-anchor-7**. Easy to picture, hard to crack.

What to avoid

- Anything a stranger could learn or guess: your name, birthday, pet's name, street, "1234," or the word "password."
- A single ordinary word, however long.
- The same password on more than one account.
- A password you've used for years on many sites — it's time to retire it.

TIP

You don't change a good password on a schedule anymore

Old advice said to change every password every few months. The experts dropped that, because it just made people pick weaker, predictable passwords. The new rule: pick a strong, unique one and *keep* it — and only change it if you have reason to think it was exposed. Less work, more safety.

CHAPTER 29

The Password Manager: A Safe That Remembers For You

If the thought of a different long password for every account makes your head spin, here is the single best tool there is — and it does the remembering for you. It's called a **password manager**, and once you have one, passwords stop being a chore forever.

What it is, in plain terms

A password manager is like a **locked safe for all your passwords**, kept on your phone and computer. You remember *one* strong password — the key to the safe (called your "master password"). The manager remembers all the rest, fills them in for you when you log in to a website, and can even invent strong new ones when you sign up somewhere. One thing to remember instead of a hundred.

WHAT THIS DOES FOR YOU

What this does for you

With a password manager you get the safety of a long, unique password on every account — the gold standard — without having to remember or type any of them. It also quietly warns you if a password is weak, reused, or caught up in a known breach. It turns the hardest part of online safety into something automatic.

Which one to use

There are several trustworthy choices, and you likely already own one for free:

- **The one built into your phone or browser.** Apple devices have **iCloud Keychain** (now a "Passwords" app); Google/Android and the Chrome browser have **Google Password Manager**. These are free, built in, and perfectly good for most folks.
- **A dedicated app** such as Bitwarden, 1Password, or similar, if you want one that works the same across every kind of device. Some are free; others cost a few dollars a month.

FROM BILL

Start with the one you already have

You don't need to buy anything to begin. The password manager built into your phone is a fine place to start, and it's probably already offering to save your passwords when you log in. If you'd like, I'm glad to sit down and set one up with you properly, so it feels easy from day one. That's exactly the kind of thing worth doing together once.

CHAPTER 30

Using a Password Manager, Step by Step

Let's make this concrete. The exact wording differs a little between phones and apps, but the idea is always the same, and it's genuinely simple once you've done it once.

Setting it up

1. Decide which manager to use (the built-in one on your phone is the easy start).
2. Create your **one master password** — make it long and memorable using the three-words trick, and this is the one to write down and keep safe at home.
3. If it offers to turn on **Face ID** or **fingerprint** unlocking, say yes — then your face or thumb opens the safe day to day, and the master password is your backup.

Saving passwords as you go

From now on, when you log in to a website or app, your manager will pop up and ask, "Save this password?" Say **yes**. Over a few weeks, as you visit your usual sites, the manager quietly collects them all — no big one-time chore. When you sign up for something new, let it **suggest a strong password**; it'll remember it so you never have to.

Logging in afterward

1. Go to the website or open the app as usual.
2. When the login boxes appear, your manager offers to fill them — confirm with your face, thumb, or master password.
3. You're in, without typing or remembering a thing.

HEADS UP

Guard the master password like a house key

Your master password is the one key to the whole safe, so give it the care it deserves: make it long, never reuse it anywhere else, and write it on a card kept somewhere private at home (not stuck to the computer). If you forget it, some managers genuinely cannot recover it — so that written backup matters.

CHAPTER 31

Prefer Paper? The Password Book Done Safely

Not everyone wants an app, and that's perfectly all right. A simple notebook of passwords can be safe — far safer than reusing one weak password everywhere — as long as you follow a few sensible rules. Let's do it properly.

The rules for a safe password book

- Use a **dedicated little notebook** (you can buy ones labeled "password book" with alphabet tabs, or just use any notebook).
- Write **neatly** and in **pencil**, so you can update entries. Note the website, your username, and the password for each.
- Keep it **somewhere private at home** — a drawer, not taped to the computer and not in your purse or wallet where it could be lost or stolen.
- Don't label it "PASSWORDS" on the cover in big letters. A plain notebook draws no attention.
- Tell one trusted family member *where* it is, in case of emergency — but not what's in it unless needed.

TIP

Paper has one real advantage

A paper book can't be hacked over the internet — no crook on the other side of the world can reach your kitchen drawer. The only risks are losing it or someone in your home misusing it, and both are easy to manage. If paper is what makes you comfortable enough to use strong, unique passwords, then paper is the right choice for you.

HEADS UP

The one thing paper can't do

A notebook won't warn you if a password turns up in a data breach, and it won't type the password for you. That's the trade. Many folks happily keep a paper book *and* let their phone's built-in manager fill things in — belt and suspenders. Use whatever keeps you safe and calm.

CHAPTER 32

Two-Factor: The Deadbolt on Your Accounts

Here is the single strongest thing you can do to protect an important account, after a good password. It has a clumsy name — **two-factor authentication** (sometimes "two-step verification" or "2FA") — but the idea is simple and the protection is enormous.

What it means

Think of your password as the doorknob lock and two-factor as the **deadbolt**. With it turned on, logging in needs *two* things: something you **know** (your password) and something you **have** (your phone). After you type your password, the service sends a short code to your phone, or pings an app, and you confirm. Even if a crook somehow has your password, they can't get in without *your phone in their hand*.

WHAT THIS DOES FOR YOU

Why this matters so much

Two-factor stops the overwhelming majority of account break-ins, because stealing a password is common but stealing your actual phone at the same moment is not. Turning it on for your email and your bank is perhaps the highest-value ten minutes you'll spend on your safety. It's the deadbolt — and it's free.

The kinds you'll meet

Type	How it works
Text message code	The service texts you a 6-digit code to type in. The most common kind, and a big step up from no deadbolt at all.
Authenticator app	A small free app (like Google Authenticator or your password manager) shows a code that changes every 30 seconds. A bit safer than text.
Tap to approve	The service sends a "Was this you? Yes/No" prompt to your phone — you just tap Yes. Simple and secure.

STAY SAFE

The code is for YOUR eyes only

Everything in Part 2 bears repeating here: that two-factor code is a key to your account. **Never read it aloud or type it anywhere because someone asked you to.** The service sends it so *you* can log in — never so you can tell it to a caller. Anyone asking for your code is trying to break in.

CHAPTER 33

Turning On Two-Factor, Step by Step

Let's switch on the deadbolt for your most important accounts. The wording varies by service, but the path is nearly always the same, and you only do it once per account.

The general steps

1. Log in to the account (your email first — it's the most important).
2. Find **Settings**, then look for **Security** or **Sign-in & security**.
3. Look for **Two-factor authentication**, **Two-step verification**, or **2FA**, and choose to turn it on.
4. Pick how you'd like to receive the code — a text to your phone is the simplest to start.
5. Enter the test code they send to confirm it's working. Done.

Start with these accounts

- Your **email** — the master key, so protect it first.
- Your **bank** and any financial apps.
- Any account with your card saved — Amazon, Apple, Google, PayPal.
- Social media like Facebook, so no one can hijack it.

GOOD TO KNOW

Save your "backup codes"

When you set up two-factor, many services give you a list of one-time **backup codes** to use if you ever lose your phone. Print them or write them in your password book and keep them safe at home. They're your spare key — a great comfort if you ever change phones or misplace one.

FROM BILL

This is a perfect thing to do together

Turning on two-factor for your key accounts is exactly the kind of once-and-done task that's easier with a patient person beside you — so you're sure it's set up right and you understand it. If you'd like, call me at (330) 200-8042 and we'll walk through your important accounts in one calm sitting.

CHAPTER 34

Passkeys, Face ID & Fingerprint Login

The newest way to log in does away with typing a password at all — and it's both easier and safer. You may already be using part of it without knowing the name.

Face and fingerprint unlocking

Many phones and computers let you log in with your **face** or **fingerprint** instead of typing. Your face or thumbprint never leaves your device — it simply unlocks the password or key already stored there. It's wonderfully convenient and very secure, because a crook can't type in your face. If your device offers it and your hands and eyes are comfortable with it, it's well worth using.

Passkeys — the password's replacement

A **passkey** is a newer kind of login that replaces the password entirely. Instead of a secret you type, your device holds a secure key, and you approve logins with your face, fingerprint, or device PIN. Because there's no password to steal and nothing to type into a fake page, passkeys can't be phished — which makes them one of the safest options there is. More and more websites now offer them.

WHAT THIS DOES FOR YOU

Nothing to remember, nothing to steal

Passkeys are a rare case of "more secure" and "easier" at the same time. There's no password to forget, reuse, or hand to a crook by mistake. When a site you use offers to set up a passkey, it's usually worth saying yes — though it's perfectly fine to keep using strong passwords plus two-factor if you prefer what you know.

TIP

You can keep it simple

Don't feel you must rush to passkeys. A strong, unique password plus two-factor on your important accounts is excellent protection and will serve you well for years. Passkeys are a nice bonus to adopt gradually, one account at a time, whenever a site invites you.

CHAPTER 35

Recovery, Security Questions & Keeping the Keys

A few loose ends make the difference between "locked out and panicking" and "calmly back in." Let's tie them up so your accounts are not just protected, but recoverable.

Keep your recovery details current

Most accounts let you set a **recovery email** or **recovery phone number** — where they send help if you're locked out. Make sure these are *yours* and up to date. If you change your phone number or email, update it in your important accounts, or you may find yourself unable to get back in later.

Security questions: a quiet weak spot

Those "security questions" — mother's maiden name, first pet, street you grew up on — are weaker than they look, because the answers can often be found online or guessed. If a site makes you set them, you're allowed to give **fake but memorable** answers (store them in your password manager or book). Your first pet can be "BlueTractor42" as far as the website knows — a crook will never guess that.

STAY SAFE

Plan for your "what if"

Think, calmly, about what would happen if you lost your phone or forgot your master password tomorrow. Written-down backup codes, a recovery email you can reach, and one trusted family member who knows where your password book lives — those three things turn a disaster into a minor inconvenience. Set them up now, while it's quiet.

FROM BILL

Leaving the keys for your family

It's a kindness to your loved ones to make sure someone you trust can get into your important accounts if something happens to you — your email, your bank, your photos. A sealed note with your password book's location, kept with your other important papers, is a thoughtful, simple way to do it. I'm glad to help you set this up sensibly if you'd like.

PART 4

Your Devices, Kept Safe

Your phone, tablet, and computer come with strong protections built right in. A handful of simple habits — mostly "let it do its job" — keeps them tidy and safe without any fuss or expensive extras.

CHAPTER 36

Your Devices Are Safer Than You Fear

Before we touch a setting, let me ease a worry. Modern phones, tablets, and computers are built with a great deal of protection baked in from the factory. They are not fragile, and they are not sitting ducks. Most of "securing your device" is simply letting those built-in protections do their work — and not getting tricked into switching them off.

Where the real risk lives

Here's the honest truth after decades of doing this: the biggest danger to your device isn't some mysterious hacker breaking in from afar. It's a person being **tricked** into opening the door themselves — installing a bad program, giving a "support" caller remote control, or typing a password into a fake page. In other words, the scams from Part 2 are the real threat, and you've already learned to beat those. The device itself is largely on your side.

WHAT THIS DOES FOR YOU

Mostly, you just let it protect you

The good news running through this whole part: safety on your devices is less about fiddling with settings and more about a few calm habits — keep it updated, lock the screen, only install from the right place, and don't be talked into turning protections off. Do those, and your device takes care of the rest.

CHAPTER 37

The Single Best Habit: Keep It Updated

If you do only one thing for your device's safety, make it this: **let it install its updates.** Those little "Update available" messages aren't nagging you for no reason — they're how the company fixes newly-found weak spots before crooks can use them.

What updates actually do

An update (sometimes called a "software update" or "security patch") is the maker — Apple, Google, Microsoft — sending your device repairs and improvements. Many of those repairs close security holes. Skipping updates for months leaves those holes open. Installing them is like a locksmith coming by for free to fix a lock that was found to be pickable.

TIP

Turn on automatic updates and forget about it

The easiest path is to let your device update **automatically**, usually overnight while it charges. On most phones this lives in Settings under "Software Update" or "System Update" — turn on "Automatic Updates." Then you never have to think about it again; it quietly keeps itself safe.

Don't forget the apps and the computer

- Your **apps** update too, through the App Store (Apple) or Play Store (Android). Let these update automatically as well.
- Your **computer** (Windows or Mac) does the same — let it install updates when it asks, and restart when it wants to. It only takes a few minutes.
- Your **internet box** (router) and smart gadgets get updates too; most do it themselves, but it's worth knowing they exist.

HEADS UP

A fake update is a trick — a real one never arrives by pop-up ad

Real updates come from your device's own Settings, or from the App/Play Store — never from a flashing web pop-up shouting "Your Flash Player is out of date, click to update!" Those are scams that install bad software. If a web page tells you to update something, ignore it and check Settings yourself instead.

CHAPTER 38

The Lock Screen: Your Device's Front Door

The simplest physical protection for your phone or tablet is a **lock screen** — the code, face, or fingerprint needed to open it. It means that if your device is lost or stolen, a stranger can't simply pick it up and get into your email, photos, and bank.

Set a lock, and make it a good one

- Use at least a **6-digit PIN** rather than 4, and avoid obvious ones like "123456," "000000," or your birth year.
- Turn on **Face ID** or **fingerprint** if your device offers it — then you rarely type the code, but it's there as backup.
- Set the screen to **lock itself** after a minute or two of no use, so it's never left open on a table.

WHAT THIS DOES FOR YOU

A locked phone is a locked diary

Think of everything your phone holds: messages, photos, your banking app, your email. A lock screen is the cover and clasp on that diary. It takes two seconds of your day and turns a lost phone from a crisis into a mere annoyance. Well worth it.

"Find My" — locate or erase a lost device

Both Apple and Android have a free feature — **Find My** (Apple) or **Find My Device** (Google) — that lets you see where a lost phone is on a map, make it ring, lock it, or even erase it from afar so a thief gets nothing. It's worth switching on now (in Settings) so it's ready before you ever need it. I'm happy to help you turn it on.

CHAPTER 39

Antivirus: Myths, Truths & What You Actually Need

"Do I need to buy antivirus?" is one of the most common questions I get, and there's a lot of confusing (and fear-driven) marketing out there. Let me give you the plain, honest answer, which will likely save you money.

Phones and tablets

For **iPhones and iPads**, you do *not* need to buy antivirus — Apple's design doesn't allow traditional viruses, and those "your iPhone is infected!" pop-ups are always fake. For **Android** phones, the built-in Google Play Protect guards you well, as long as you only install apps from the Play Store. You can skip the paid "phone cleaner" apps — many are junk or worse.

Computers

- **Windows** computers come with **Windows Security** (also called Microsoft Defender) built right in, turned on, and free. For most folks it's all you need — no purchase required.
- **Macs** have strong built-in protection too, and most Mac users get along fine without buying anything extra.

GOOD TO KNOW

The best antivirus is your own caution

Here's the truth the ads won't tell you: no antivirus program protects you as well as the habits in this book. Viruses today mostly arrive because someone was *tricked* into installing something or giving access. The built-in protection plus your own good judgment beats any expensive package. Save your money.

HEADS UP

"Antivirus" pop-ups and calls are often the scam

Beware: many "antivirus" and "PC cleaner" pop-ups and calls are themselves the scam — they frighten you into installing the very thing that causes trouble, or into paying for a "subscription" you don't need. Stick to the protection already built into your device, and ignore the scary ads.

CHAPTER 40

Scary Pop-Ups & Suspicious Downloads

We met the tech-support pop-up back in Part 2; here we'll make you completely comfortable with pop-ups in general, so none of them can rattle you again.

What a pop-up really is

A pop-up is just a little window that a web page opens. However loud, flashing, or alarming it looks — sirens, countdown timers, "DO NOT CLOSE THIS WINDOW" — it is only a web page, with no power over your device unless *you* act on it. It cannot actually see a virus, and it cannot harm you if you simply walk away from it.

How to clear any pop-up

1. Don't call any number and don't click the buttons inside the pop-up (even an "X" inside it can be a trick).
2. Close the browser tab or window. If it won't let you, close the whole browser program.
3. If it still won't budge, **restart the device** — turn it fully off and on. That clears any web pop-up, guaranteed.
4. Carry on with your day. Nothing was infected; it was a bluff.

STAY SAFE

Only download from the right places

Programs and apps should come from **official stores only**: the App Store on Apple, the Play Store on Android, and — on a computer — the maker's own website or the Microsoft/Mac store. Never install something a pop-up, email, or stranger urges on you. "Free" programs from unknown websites are a common way trouble sneaks in.

FROM BILL

When in doubt, don't click — ask me

If a download, a pop-up, or a "you must install this" message leaves you unsure, the safe move is to do nothing and ask. A quick call to (330) 200-8042 costs you nothing and can save a real headache. I would far rather you call me about ten harmless things than click one harmful one.

CHAPTER 41

Public Wi-Fi: Coffee-Shop & Airport Safety

"Is it safe to use the free Wi-Fi at the coffee shop, the library, the airport?" A fair question, and the answer is reassuring with one or two sensible habits.

The simple truth

Public Wi-Fi is fine for ordinary browsing — reading the news, checking the weather, looking things up. The one caution is that, on a shared network, it's *possible* (though far less common than it used to be) for the connection to be snooped on. So the sensible habit is simply about *what* you do on it.

The habits

- On public Wi-Fi, happily browse, but **save your banking and shopping** for home, or do them using your phone's own cellular data instead.
- If you must bank on the go, use your phone's **mobile data** (the cellular signal) rather than the café's Wi-Fi — it's private to you.
- Beware networks with odd names pretending to be the venue's ("Free Airport WiFi!!"). When unsure, ask the staff for the real network name.
- Modern banking and shopping sites are themselves encrypted (that little padlock we'll cover in Part 5), which adds strong protection even on shared Wi-Fi.

GOOD TO KNOW

Your phone's data is your private tunnel

When you're out and about, your phone's own cellular connection (the signal that makes calls) is private to you — nobody at the café shares it. So for anything sensitive on the go, turning Wi-Fi off and using your mobile data is a simple way to stay private. For big jobs, wait until you're home on your own network.

CHAPTER 42

Your Home Wi-Fi & Internet Box

Your home internet comes through a box called a **router** (sometimes combined with the modem). It's the front gate to your home network, and a couple of one-time settings make it nicely secure. You set these once and forget them.

The two settings that matter

- **A strong Wi-Fi password** so neighbors and passers-by can't hop on your network. Most routers come with a random one printed on a sticker — that's fine — but if yours is simple, change it to something strong.
- **Change the router's *admin* password.** This is a separate password that controls the router's own settings, and it often ships as "admin/admin" or "password." Changing it shuts a door crooks sometimes try.

Keep it healthy

- Let the router install its own updates (most do automatically).
- Restarting the router (unplug 30 seconds, plug back in) fixes most slow or dropped connections.
- If your router is very old (say, more than five or six years), a newer one is faster and more secure — worth considering.

FROM BILL

Routers are fiddly — I set these up all the time

Router screens are genuinely confusing, with cramped menus and jargon, and you only visit them once in a blue moon. This is a very common thing I help folks with: a quick visit to set a strong password, change the admin login, and make sure it's all tidy and secure. If yours has never been touched since it was installed, it's worth a look. Just call me.

CHAPTER 43

Backing Up: So Nothing Is Ever Truly Lost

A "backup" is a second copy of your photos, messages, and files, kept somewhere safe, so that if your device is lost, stolen, broken, or locked up, your memories and documents are not lost with it. It's one of the most comforting things you can set up — and it also protects you from one nasty kind of scam.

The easy way: automatic cloud backup

The simplest backup happens by itself, over the internet, to your device maker's "cloud" (just a secure storage space on their computers):

- **Apple** devices back up to **iCloud** — turn on iCloud Backup in Settings, and it saves overnight while charging on Wi-Fi.
- **Android** devices back up to your **Google Account** — turn on backup in Settings, and photos save to Google Photos.
- **Computers** can back up to the cloud too, or to a plug-in external hard drive you keep at home.

WHAT THIS DOES FOR YOU

Backup beats ransomware cold

There's a nasty scam called "ransomware" where crooks lock up your files and demand payment to unlock them. If you have a good backup, you can simply shrug, restore your files, and owe them nothing — the threat vanishes. Beyond scams, a backup means a dropped or lost phone never costs you a single photo. Peace of mind, automated.

TIP

The best backup is the one that happens by itself

Don't rely on remembering to back up by hand — turn on the *automatic* cloud backup and let it run quietly. Once a year, it's worth confirming it's still working. If you're not sure whether yours is on, that's a fine thing to check together on a call.

CHAPTER 44

Spam Calls, Robocalls & Voicemail

The telephone is still a scammer's favorite tool, so let's tame it. You can cut down the flood of junk calls and handle the ones that get through with complete calm.

Cutting down the junk

- Register your number — for free — on the national **Do Not Call** list at donotcall.gov. It won't stop crooks (they ignore it), but it cuts legitimate telemarketing.
- Turn on your phone's **spam-call filtering**. Both iPhone and Android can silence or label calls from suspected spam numbers — look in your phone app's settings.
- Let **unknown numbers go to voicemail**. Real callers leave a message; most scammers don't bother.

When a junk call gets through

1. You owe a stranger nothing — you may hang up at once, no explanation needed.
2. Don't press buttons "to be removed" or "to speak to someone" — it just confirms a live person and invites more calls.
3. Don't say "yes" to "Can you hear me?" and similar — just hang up.
4. Never follow a recorded message's instructions to "press 1" about your account, a warrant, or a prize.

STAY SAFE

A spoofed number proves nothing

Remember from Part 1: crooks can make *any* name or number show on your phone, including your own bank's. So never trust a call just because the screen says "IRS" or shows a local number. If it matters, hang up and call back on a number you look up yourself. The caller ID is not evidence of anything.

CHAPTER 45

Smart-Home Gadgets: Cameras, Doorbells & Speakers

Video doorbells, security cameras, and voice speakers (like Alexa or Google) are wonderful for safety and convenience — and because they connect to the internet, they deserve the same few sensible habits as everything else. Nothing to fear; just a little tidiness.

Setting them up safely

- Give each gadget's app a **strong, unique password**, and turn on **two-factor** if it's offered — this is what keeps a camera feed yours alone.
- Let the gadgets install their **updates** automatically.
- Place cameras thoughtfully — pointed at your own property, not a neighbor's windows — and know what each one records.

GOOD TO KNOW

Most "hacked camera" stories are really reused passwords

You may have heard alarming tales of strangers talking through someone's camera. Almost always, that happened because the owner reused a password that had leaked from some other site — not because the camera itself was broken into. A unique password plus two-factor on the app shuts that door completely. It all comes back to Part 3.

A gentle word on voice speakers

A voice speaker listens for its "wake word" and sends what follows to the company to answer you. That's how it works, not a spy in the room — but if it bothers you, you can mute its microphone with the button on top, review and delete your voice history in its app, and keep it out of the most private rooms. You're always in control of it.

FROM BILL

Happy to help you set up a doorbell or camera right

Smart doorbells and cameras are genuinely useful for peace of mind, but the setup — the app, the password, the Wi-Fi, where to aim it — trips a lot of folks. It's one of my favorite things to help with. If you've got one in a box, or want advice on choosing one, give me a call at (330) 200-8042.

CHAPTER 46

Passing On a Device Safely: Wipe It First

When you sell, give away, trade in, or recycle an old phone, tablet, or computer, there's one step you must never skip: **erasing your personal information** from it first. Otherwise your photos, messages, and saved logins go out the door with the device.

How to erase a device

1. First, make sure everything is **backed up** (previous chapter) so you keep your photos and files.
2. **Sign out** of your accounts on the device — especially your Apple ID or Google Account, so the new owner can use it.
3. Use the device's built-in **"Erase All Content and Settings"** (Apple) or **"Factory Reset"** (Android/Windows) — this wipes it clean back to how it left the factory.
4. For a computer, the same idea: a factory reset or "reset this PC" that removes your files.

HEADS UP

Don't forget the little things

Before letting a device go, remember to remove any **SIM card** or **memory card** (little removable chips), and double-check photos and messages are backed up and the device shows as freshly reset. If you're trading in to a store, they often help — but the erasing is your responsibility, and it's easy.

FROM BILL

Old devices: erase, then recycle properly

Don't just toss an old device in the trash — it holds your data and shouldn't go to landfill. Erase it, then recycle it at an electronics drop-off or trade it in. If you've got a drawer of old phones and aren't sure how to wipe them safely, bring them along next time I visit, or give me a call — I'll make sure they're clean before they leave your hands.

PART 5

Safe on the Web

Browsing, shopping, and banking online are among the great conveniences of modern life — and they're safe once you know a few simple tells. We'll make you comfortable spotting a real site from a fake, and doing your business with confidence.

CHAPTER 47

The Padlock & "https": What "Secure" Means

Up at the top of your screen, where the website's address shows, there's a small clue about safety that's worth understanding — though, as you'll see, it means a little less than people think.

The padlock and the "s"

When a web address begins with **https** (with an "s") and shows a little **padlock** symbol, it means the connection between you and that website is **encrypted** — scrambled so that nobody in between can read what you type, like your password or card number. That's a good thing, and you want it whenever you log in or pay.

HEADS UP

The padlock means "private," not "honest"

Here's the catch most people miss: the padlock only promises the connection is *private* — it does **not** promise the website is *trustworthy*. Crooks can put a padlock on a fake site just as easily as anyone. So a padlock is necessary but not enough; you still need to be sure you're on the *real* site, which the next chapters cover.

When to insist on the padlock

- Always look for it before typing a **password**, a **card number**, or personal details.
- If a login or payment page shows "Not Secure" or no padlock, stop — don't type anything sensitive.
- For simply reading an article, the padlock matters less, but nearly all sites have it now anyway.

CHAPTER 48

Reading a Web Address Like a Pro

A web address (the "www" line at the top) tells you exactly where you are — if you know how to read it. This one small skill defeats a whole category of fakes, so let's learn it calmly. It's easier than it looks.

Find the real name: the part just before the first single slash

The true identity of a site is the word just before the **.com** (or .org, .gov) and before the first single slash **/**. Read it from that point *backwards*. For example, in **accounts.google.com**, the real site is **google.com** — the "accounts" part is just a room inside Google's house. Everything after the first slash is just pages within the site.

How crooks dress up a fake address

A real address	A crook's lookalike
amazon.com	amazon-security.com (extra words = different site)
chase.com	chase.verify-login.com (real name is verify-login.com)
paypal.com	paypa1.com (a "1" instead of the letter "l")
irs.gov	irs-refund.net (not .gov, and extra words)

GOOD TO KNOW

Tricks to watch for in an address

Crooks sprinkle in **extra words** (amazon-*support*.com), **swapped letters** (a zero for an O, a "1" for an "l"), or **wrong endings** (.net or .co instead of .com). And remember: anything after the first single slash doesn't change who owns the site. When the address looks even slightly off, don't enter anything — leave and go to the real site yourself.

TIP

".gov" is reserved for the real government

Only genuine U.S. government bodies may use web addresses ending in **.gov**. So irs.gov, ssa.gov, medicare.gov, and usa.gov are the real thing, while "irs-refunds.com" or ".net" versions are not. This is one address rule you can lean on firmly.

CHAPTER 49

Reaching a Website the Safe Way

We keep returning to one habit because it's the most protective of all: when you want to visit an important site — your bank, Amazon, the IRS — get there **under your own steam**, never through a link someone handed you. Here's how to make that effortless.

The three safe doorways

1. **Type the address yourself** in the browser's address bar — chase.com, amazon.com — carefully, watching the spelling.
2. **Use a bookmark** you saved earlier (see below). One tap, always the right place.
3. **Use the company's official app**, which you installed from the App or Play Store. The app always goes to the real site.

Make bookmarks for the sites you use most

A **bookmark** (or "favorite") is a saved shortcut to a website, so you never have to type the address or risk a typo that lands you on a fake. To make one, visit the real site, then tap the **share** or **star** symbol and choose **Add Bookmark** or **Add to Favorites**. After that, your bank is one reliable tap away.

STAY SAFE

Never log in through a link in a message

This is the golden rule, said once more because it stops so much trouble: if an email or text says "click here to log in and fix your account," **don't**. Open your bookmark, your app, or type the address yourself. Real companies never *need* you to log in through a link they sent. Going your own way makes fake links harmless.

CHAPTER 50

Spotting a Fake or Lookalike Website

Sometimes you land on a page that's *meant* to look like a company you trust. Here's how to tell a counterfeit from the real thing, using more than just the address.

The warning signs

- An **address that's off** — extra words, odd spelling, wrong ending (the last chapter's skill).
- **Spelling and grammar mistakes**, odd phrasing, or a layout that looks slightly cheap or crooked.
- It **rushes you** — countdown timers, "act now," "your account will be closed."
- It asks for **too much** — your full Social Security number, your password plus your mother's maiden name plus your PIN, all at once.
- Payment only by **gift card, wire, or crypto**, or prices far too good to be true.
- No real company address, no phone number, no way to reach a human.

GOOD TO KNOW

When in doubt, leave and start fresh

You never have to figure out for certain whether a page is fake. The safe move whenever something feels off is simply to **leave** — close the page — and reach the company your own way (type the address, use your bookmark or app). If the page was real, you've lost nothing; if it was fake, you've dodged it entirely.

CHAPTER 51

The "Support Number" Trap in Search Results

Here's a sneaky one that catches careful people, so it deserves its own chapter. It happens when you *search* for a company's phone number or help line.

How it works

Say you want to call Amazon, your printer's maker, or an airline. You type the company name plus "customer service" into a search engine. Among the results — sometimes right at the top, marked "Sponsored" (an advertisement) — sits a **fake support number** set up by crooks. You call it, and a friendly "agent" offers to help... and then asks to remote into your computer or wants a gift-card payment. It's the tech-support scam, reached through a search.

STAY SAFE

Get support numbers from the company's own site

Don't trust a phone number just because it appears in a search. Instead, go to the company's **official website** (type the address or use your bookmark/app) and find "Contact" or "Help" *there*. The number on the company's own site is the real one. The same goes for a number printed on your product, box, or bill.

HEADS UP

"Sponsored" results are advertisements

At the top of search results, entries marked **Sponsored** or **Ad** are paid placements, and crooks sometimes buy them to impersonate real companies. Scroll past the ads to the ordinary results, and better still, go straight to the company's own site. Treat a phone number in a sponsored result with real caution.

CHAPTER 52

Safe Online Shopping, Start to Finish

Shopping online is one of the genuine joys of the internet — especially when getting out is harder than it used to be. The vast majority of it is perfectly safe. Here's how to keep it that way, from browse to doorstep.

Before you buy

- Prefer **well-known stores** or their official apps. For a shop you don't know, search its name plus "reviews" or "scam" first.
- Make sure the page is **secure** (padlock) and the address is the real store.
- Be wary of deals that are **far** cheaper than everywhere else, and of ads on social media leading to unknown shops.

Paying safely

- **Pay by credit card** whenever you can — it carries the strongest protection if something goes wrong, letting you dispute a charge.
- Avoid paying a store by **debit card, wire, gift card, money app, or crypto** — these have little or no protection.
- Never send money to a private seller you can't verify; for local pickups, cash in a public place is simplest.

WHAT THIS DOES FOR YOU

A credit card is your safety net

The single best shopping habit is to pay by credit card. If goods never arrive, or a store turns out to be a fraud, or your number is stolen, your card company can dispute the charge and you're generally not on the hook. It's a powerful, free protection — use it for all your online buying.

After you buy

- Keep the **confirmation email** until the item arrives and you're happy with it.
- Track the package through the **store's own site or app** — never through a surprise "delivery problem" text (that's the smishing scam).
- Check your card statement now and then for charges you don't recognize.

CHAPTER 53

Safe Online Banking

Banking from your own chair, any hour, without a drive to the branch — it's wonderfully convenient, and banks have built it to be very secure. With a few habits, you can use it with complete peace of mind.

Getting in safely

- Use your bank's **official app** (from the App or Play Store) or type the bank's address yourself — never a link from an email or text.
- Give your bank login a **strong, unique password** and turn on **two-factor** (Part 3) — this is exactly the account that most deserves the deadbolt.
- On your own private phone, the banking app plus your face or PIN is both convenient and secure.

Everyday safe habits

- **Check your statements and balances** regularly — catching an odd charge early makes it far easier to fix.
- Turn on your bank's **alerts** for large or unusual transactions, so you hear about trouble fast.
- Save banking for your **home network** or your phone's cellular data, not shared public Wi-Fi.
- Log out when you're done on a **shared or public** computer.

SCAM ALERT

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

This bears repeating in the banking chapter because it steals so much: no real bank ever phones to say your account is under attack and you must move your money to a "safe" or "holding" account, or send it to yourself. That is always the scam. If a "bank" caller says anything like it, hang up and call the number on the back of your card.

FROM BILL

Online banking is safer than most people fear

Many folks worry online banking is risky, but with a strong password, two-factor turned on, and the habit of reaching your bank your own way, it's genuinely safe — often safer than carrying cash or mailing checks. If you'd like to set it up together so you feel sure of it, that's a wonderful thing to do once. Just call.

CHAPTER 54

Email Safety: A Closer Look

Email is where a great many scams arrive, and it's also your most important account (the master key, remember). A little care with your inbox goes a very long way.

Reading email with a calm, careful eye

- Check **who really sent it**: tap the sender's name to see the actual email address. "Amazon" from "security@amaz0n-alerts.ru" is a fake.
- Be suspicious of **urgency and threats**, unexpected attachments, and requests for passwords or payment.
- A greeting of "Dear Customer" rather than your name is a common sign of a mass scam.
- When an email about an account worries you, don't click it — open that account your own way and check.

Keeping your inbox tidy and safe

- Use your email's **Spam** or **Junk** button on scams — it teaches your email to catch more of them.
- Don't "unsubscribe" from obvious scam email — like pressing 1 on a robocall, it just confirms you're real. Just delete or mark as spam.
- Give your email account a strong, unique password and two-factor — it protects everything else.

GOOD TO KNOW

One email address, used wisely

It can help to keep your main email address for people and important accounts, and use it sparingly when signing up for newsletters, contests, or shops. The less widely your address is spread around, the less scam mail finds you. Some folks keep a second, "junk" address just for sign-ups — a tidy trick if you'd like one.

CHAPTER 55

Links & Attachments: Look Before You Leap

Two things in a message deserve special care, because they're how most trouble sneaks in: **links** (words or buttons you tap to go somewhere) and **attachments** (files stuck to an email). Treat both with a calm, questioning eye.

Links: see where they really go

A link can *say* one thing and *go* somewhere else entirely. On a computer, you can rest your mouse pointer over a link *without clicking*, and the real destination appears at the bottom of the screen. On a phone, press and hold the link gently to peek at where it leads. If the address isn't what you'd expect, don't tap it.

Attachments: only open what you expect

- Open an attachment **only** if you were expecting it from someone you know and trust.
- Be especially wary of attachments in unexpected emails — a "receipt," an "invoice," a "photo" from a stranger. These can carry viruses.
- If unsure whether an attachment from a friend is genuine, ask them (another way) before opening it — their email may have been hacked.

STAY SAFE

When in doubt, don't tap — go the long way

You never lose anything by *not* tapping a link or opening an attachment. If the message might be real, reach the company or person your own way and check. A moment's caution costs nothing; a careless tap can cost a great deal. Slow and sure wins here, every time.

CHAPTER 56

Your Browser Is on Your Side

The program you use to visit websites — Safari, Chrome, Edge, or Firefox — is called a **browser**, and it quietly does a lot to keep you safe. Knowing its helpers makes you feel more in control.

Built-in protections you already have

- **Dangerous-site warnings**: if you're about to visit a known scam or malware site, your browser throws up a big red warning. When it does, **heed it** — back away.
- **The padlock and address bar** show whether a connection is secure and where you really are.
- **Pop-up blocking** stops most unwanted pop-up windows automatically.
- **Automatic updates** keep the browser patched — another reason to let updates run.

HEADS UP

When the browser shows a red warning, believe it

A full-page red warning that says "Deceptive site ahead" or "This site may harm your computer" is your browser protecting you — not a scam. Don't click through to "proceed anyway." Simply go back. Your browser rarely cries wolf, so when it warns you, trust it.

TIP

One browser, kept simple

You don't need several browsers or a pile of "add-ons." One trustworthy browser, kept updated, with its built-in protections on, is all most folks need. Fancy extra toolbars and "helpers" you're urged to install are often more trouble than they're worth — keep it clean and simple.

CHAPTER 57

Cookies, Ads & Those "Accept" Boxes

If the words "cookies" and "trackers" make the web feel vaguely sinister, let me demystify them. They're mostly ordinary, mostly harmless, and easy to handle calmly.

What a "cookie" actually is

A **cookie** is just a small note a website leaves on your device to remember you — so you stay logged in, or your shopping cart isn't empty when you come back. Most cookies are helpful and harmless. Some are used by advertisers to notice which sites you visit, which is why you sometimes see an ad "follow" you around. A nuisance, not a danger.

Those "Accept Cookies" pop-ups

Many sites now greet you with a box about cookies, because the law requires them to ask. You can simply click **Accept** to get on with it, or look for **Reject** or "Necessary only" if you'd rather share less. Either choice is safe — it's not a scam, just a legal formality. Don't let it worry you.

GOOD TO KNOW

Ads are annoying, not dangerous — but don't click wild ones

Ads pay for many free websites, so you'll see plenty. They're not harmful in themselves, but treat flashy ones — "You've won!", "Your device is infected!", "One weird trick!" — exactly like scam pop-ups: don't click them. Scroll past, and get what you came for from the real content.

CHAPTER 58

Safe Video Calls With Family

Seeing a grandchild's face while you talk is one of the true gifts of modern technology, and video calling — on FaceTime, Zoom, Facebook Messenger, WhatsApp, and the like — is safe and lovely once you know a couple of small things.

Keeping video calls safe and comfortable

- **Only accept or join calls from people you know.** You don't have to answer a video call from a stranger any more than a phone call.
- For group meetings (like a Zoom), don't share the meeting link or code publicly, so uninvited folks can't wander in.
- If a call ever feels wrong — someone pressuring you, or a "relative" who looks or sounds slightly off — you can hang up and call them back on their known number.
- Install these apps only from the official App or Play Store, never from a link.

HEADS UP

Faked faces and voices are rare, but call back if unsure

You may have heard that crooks can now fake a person's voice or even video. It's uncommon, and it still can't survive your old reliable habit: if anything about a call feels off, or it turns to money or secrecy, hang up and reach your loved one on the number you already have. A real family member will never mind.

WHAT THIS DOES FOR YOU

Worth every minute of setting up

Of all the things technology offers, seeing your family face to face from your own chair may be the dearest. If video calling feels daunting, it's absolutely worth learning — and it's one of the happiest things I help folks set up. Once it works, it tends to become a weekly joy.

CHAPTER 59

When a Site Asks to Install, Allow, or Notify

Now and then a website asks for permission to do something — show you notifications, use your location, or install a program. A moment's thought before you tap "Allow" keeps you tidy and safe.

The common requests, and how to answer

What the site asks	How to answer
"Allow notifications?"	The site wants to send you pop-up alerts. Usually say No/Block — few sites truly need this, and crooks abuse it to send scam alerts later.
"Allow your location?"	Fine for a maps or weather site you trust; otherwise Don't Allow. It's rarely needed just to read a page.
"Install this program/extension"	Be cautious. Only install software you went looking for, from the maker's own site — never because a page pushed it on you.
"Open this file?"	Only if you deliberately chose to download it from a trusted place. If a page tried to download something by itself, decline.

STAY SAFE

"Allow" is a door — open it only on purpose

Every "Allow" or "Install" button opens a little door into your device. There's no harm in saying **No** or **Block** to any of them — you can always allow it later if you find you need to. When a page you didn't trust asks for permission, the safe answer is almost always no.

FROM BILL

Those browser notification pop-ups trip a lot of folks

A very common one I get called about: someone clicked "Allow" on a notification request months ago, and now scary alerts pop up on their screen and they think they're hacked. They're not — it's just that permission, and it's easily switched off in the browser's settings. If this is happening to you, don't worry, and give me a ring; it's a two-minute fix.

PART 6

Your Private Information

Your personal details are valuable — to you, and to crooks. This part is about keeping a sensible grip on what you share, understanding why you get so many scam calls, and taking a few powerful steps that lock the door before trouble ever starts.

CHAPTER 60

Why Your Information Is Worth Protecting

Your name, birthday, address, phone number, Social Security number, and account details are the raw materials of "identity theft" — where a crook uses your information to open accounts, borrow money, or claim benefits in your name. The more pieces they gather, the more harm they can do. So a little care about what you share is genuinely protective.

Not all information is equal

You don't need to lock everything away or stop living online — that's no life at all. The trick is knowing which pieces matter most, and guarding *those* closely while being relaxed about the rest.

Sensitivity	What belongs here
Guard very closely	Social Security number, Medicare number, full card and account numbers, passwords, PINs, two-factor codes.
Share with care	Date of birth, home address, mother's maiden name, phone number — handy to crooks, so don't scatter them freely.
Fairly harmless	First name, the town you live in, your interests and hobbies — the ordinary stuff of being sociable.

WHAT THIS DOES FOR YOU

A sensible grip, not a locked vault

The aim here isn't to make you anxious about every detail — it's to help you spend your caution where it counts. Guard the handful of truly sensitive items, stay a little thoughtful with the middle group, and relax about the rest. That balance keeps you safe *and* keeps life enjoyable.

CHAPTER 61

What's Safe to Share, and What Isn't

Let's turn that into everyday rules you can apply without thinking hard — whether you're filling in a form, chatting online, or answering a question from a stranger.

Good default habits

- **Never** give your Social Security number, Medicare number, full card number, password, or a texted code to anyone who contacted *you*.
- When a form or website asks for sensitive details, ask yourself: **do they really need this?** A newsletter doesn't need your birthday; a contest doesn't need your Social Security number.
- It's fine to give a store your email and maybe a phone number — but you don't owe anyone your life story to make a purchase.
- You're allowed to say **no**, or to leave optional fields blank, or to give minimal answers. Businesses ask for more than they need all the time.

TIP

"Why do you need that?" is a perfectly polite question

If a caller, clerk, or website asks for something sensitive, you may always ask why they need it and whether it's required. An honest organization won't mind explaining. Pushback or evasiveness is itself a warning sign. You are in charge of your own information — asking is your right, not rudeness.

CHAPTER 62

Oversharing on Social Media

Social media is lovely for staying close to family — and a quiet gold mine for crooks, who read public posts to learn about you. A few gentle habits let you enjoy sharing without handing strangers the keys.

What crooks look for in your posts

- **Answers to security questions** — your pet's name, your first car, your hometown, your mother's maiden name — all often asked by banks, and all often posted for fun in those "get to know me!" quizzes.
- **When you're away from home** — "Off to Florida for two weeks!" tells a burglar your house is empty.
- **Your full birthday, address, and phone number** — pieces of the identity-theft puzzle.
- **Photos that reveal your routine** or your home's layout and valuables.

Simple sharing habits

- Set your posts to **Friends only**, not Public, so strangers can't read along.
- Post about the trip **after** you're home, not while you're away.
- Skip the fun "quizzes" that ask for your first pet, first car, or street you grew up on — those are often harvesting security answers.
- Think before sharing anything you'd not want a stranger to know.

GOOD TO KNOW

Check your privacy settings once, calmly

Most social sites let you choose, in Settings, who can see your posts, your friends list, and your details. It's worth a one-time look to set these to "Friends" and tuck away your birth year and contact details. My Facebook manual walks through this step by step — or I'm glad to do it with you on a visit.

CHAPTER 63

Data Brokers & Why the Scam Calls Come

Ever wonder how scammers got your number, your age, or knew you'd recently had a birthday? You're not imagining it, and it's not because you did anything wrong. Let me pull back the curtain, because understanding it takes away the spooky feeling.

The quiet business of selling your details

There are companies called **data brokers** whose entire business is gathering facts about people — from public records, store loyalty cards, online sign-ups, and more — and selling those lists. Much of your name, age, address, and phone number sits in these databases, and crooks buy or steal such lists to find targets. It's how a scam call can "know" a little about you and sound more convincing.

GOOD TO KNOW

Them knowing a detail doesn't make them real

Scammers often open with a true fact — your name, your address, the last four digits of a card — to seem legitimate. Don't be fooled: that information is cheap and widely traded. A caller knowing your address proves nothing about whether they're genuine. The rule stands: verify independently, never act on the call itself.

Why this matters for your calm

Knowing about data brokers does two things. It frees you from feeling personally watched or singled out — you're simply on a list, like millions of others. And it points to a real step you can take to quiet the flood, which is the very next chapter.

CHAPTER 64

Shrinking Your Footprint

You can't vanish from the internet entirely, and you don't need to. But you *can* take a few steps that meaningfully reduce the junk calls, scam mail, and exposure. Think of it as tidying, not hiding.

Practical steps that help

1. Register on the national **Do Not Call** list (donotcall.gov) and turn on your phone's spam filtering — this cuts legitimate telemarketing and labels likely scams.
2. Opt out of pre-screened credit and insurance offers (the junk-mail kind) for free at **optoutprescreen.com**, run by the credit bureaus.
3. Be sparing with your real email and phone when signing up for things; use a "junk" email for sign-ups if you like.
4. Ask the big **data broker** sites to remove your listing — many have an opt-out page (search the broker's name plus "opt out"). There are also paid services that do this for you, though you can do it yourself for free.

TIP

Small steps, real quiet

You won't stop every call or letter, and chasing perfection isn't worth your afternoons. But a handful of these steps — the Do Not Call list, spam filtering, the prescreen opt-out — noticeably thins the flood over a few weeks. Do the easy ones and let the rest go.

FROM BILL

I can help you tidy up your footprint

Working through opt-outs and privacy settings is fiddly and a bit tedious — a perfect sit-down task to do together, so it's done properly once. If the scam calls and junk have been getting you down, give me a call; we'll quiet things down and you'll feel the difference.

CHAPTER 65

Handling Any Caller With Confidence

The telephone is where a lot of pressure lands, so let's give you a calm, repeatable way to handle *any* caller — known or unknown, friendly or forceful. Once you have this, no call can rattle you.

The golden phone habits

- You never have to answer an unknown number; let it go to voicemail.
- If you do answer and anything feels off, you may **hang up at any time** — no explanation owed, even mid-sentence.
- Never give sensitive details to someone who called *you*. If the matter might be real, say you'll call back on a number you look up.
- Don't be moved by urgency, threats, or flattery — those are pressure tactics, not reasons.
- Beware "Can you hear me?" and other questions fishing for a recorded "yes."

A script for the tricky moment

When a caller presses you, having words ready keeps you steady. Any of these will do, and then you hang up:

- "I don't handle anything financial over the phone. I'll call your main number myself."
- "I never give out that information on a call I didn't place. Goodbye."
- "Thank you, I'll check with my family and the bank first."

STAY SAFE

Resistance to you hanging up is the proof

Here's your reliable tell: if a caller fights to keep you on the line — "don't hang up," "stay with me," "there's no time" — that resistance *is* the evidence it's a scam. A genuine caller is always happy for you to call back and verify. Only crooks need you right now. So when they push, that's your cue to put the phone down.

CHAPTER 66

Guarding Your Most Sensitive Numbers

A few numbers deserve special protection, because they unlock the most harm. Let's be clear about which ones and how to treat them, so you never second-guess yourself.

The numbers to protect most

Number	How to treat it
Social Security number	Give it only when truly required (taxes, employment, a bank you chose). Don't carry the card; never say it to an incoming caller.
Medicare number	Treat like a credit card. Only your chosen doctors and providers need it. Medicare won't call you for it.
Card & bank account numbers	Only enter on the real company's secure site or app, or give to a business you called. Never to an incoming caller or a link.
Passwords & PINs	Never share with anyone, ever — not family "just in case" over the phone, not a "support" agent, nobody.
Two-factor codes	For your eyes only. Never read aloud or type in because someone asked.

HEADS UP

Shred the paper trail

Crooks still dig through trash and steal mail. Shred anything with account numbers, your Social Security number, or medical details before throwing it out, collect your mail promptly, and consider a locking mailbox. Old-fashioned, but identity theft often starts with a discarded statement or a stolen pre-approved credit offer.

CHAPTER 67

Freezing Your Credit: The Strongest Lock

Here is one of the most powerful protections against identity theft, and hardly anyone knows about it. It's free, it's reversible, and it slams the door on crooks trying to open accounts in your name. It's called a **credit freeze**.

What a credit freeze does

When a crook tries to open a loan or credit card in your name, the lender first checks your "credit file" at the credit bureaus. A **freeze** locks that file, so no new lender can look — which means no new account can be opened in your name, by you *or* a crook, until you lift it. Since you rarely open new credit, keeping it frozen is a small inconvenience for a big protection.

How to set one up

1. You freeze your file at **each of the three credit bureaus** separately — Equifax, Experian, and TransUnion. All three must be frozen for full protection.
2. Go to each bureau's official website (search the bureau's name, or start at the government's guide) or call them; freezing is **free by law**.
3. They'll give you a PIN or login to **lift (thaw)** the freeze later — keep it safe. You can thaw temporarily whenever you genuinely need new credit.

WHAT THIS DOES FOR YOU

Free, reversible, and quietly powerful

A credit freeze is perhaps the single best identity-theft protection there is, and it costs nothing. It doesn't affect your existing cards or your credit score, and you can thaw it any time you want to apply for something. For most of us, who open new credit rarely, keeping all three frozen is wonderful peace of mind.

FROM BILL

Setting up all three is a great thing to do together

Freezing your credit at all three bureaus, and safely storing the PINs, is exactly the kind of once-and-done protection worth doing right. It's a bit tedious solo. If you'd like a hand — and help keeping the login details somewhere safe — call me at (330) 200-8042 and we'll knock it out in one sitting.

CHAPTER 68

Keeping an Eye on Things

Protection is strongest when you also keep a gentle eye out — not anxiously, just a regular glance so you'd notice trouble early. Catching something in week one is far easier to fix than catching it in month six.

Your simple monitoring routine

- **Glance at your bank and card statements** each month for charges you don't recognize — even small ones, which crooks use to test a stolen card.
- Turn on **account alerts** from your bank and card company for large or unusual activity.
- Check your **free credit reports** once in a while at **annualcreditreport.com** (the one official free source) for accounts you didn't open.
- Read the **statements Medicare and your insurer send** for services you never received.

GOOD TO KNOW

annualcreditreport.com is the real, free one

You're entitled to free credit reports from the three bureaus, and the one genuine site for them is **annualcreditreport.com**. Beware lookalike sites and ads promising "free" reports that actually sign you up for paid services. Type that address yourself, and ignore the imitators.

TIP

A glance, not a worry

This isn't about living in fear or checking fifty times a day. A calm monthly look at your statements and an occasional credit-report check is plenty. Set a regular time — say, when you pay the bills — and it becomes a painless habit that quietly keeps you a step ahead.

CHAPTER 69

Family, Caregivers & Shared Devices

Privacy at home has its own gentle considerations — helping a family member, sharing a tablet, or letting someone assist with your accounts. A little clarity keeps trust and safety both intact.

Sharing devices sensibly

- On a **shared computer or tablet**, log out of your personal accounts when you're done, or set up separate user profiles so each person's things stay their own.
- Keep your passwords yours — even with family, share them only when there's a real need, and change them afterward if you'd rather.
- If grandchildren use your device, a little supervision and the official app stores keep things safe.

Trusted help, done right

It's wise to have **one trusted person** who could step in if you were ever unwell — knowing where your password book lives, able to reach your email and bank. That's prudent planning, not a loss of independence. Choose someone you trust completely, and consider speaking with your family or attorney about formal arrangements (like a power of attorney) for the bigger picture.

STAY SAFE

Sadly, not all fraud comes from strangers

I'll say this gently but honestly, because it matters: some financial abuse of older adults comes from people they know — a relative, a caregiver, a new "friend." Keeping your own grip on your passwords and accounts, and having more than one trusted person aware of your finances, protects you here too. If something ever feels wrong, you can always talk to me, your bank, or Adult Protective Services, in complete confidence.

FROM BILL

Set up trusted help calmly, before it's needed

The best time to arrange who can help with your accounts is when all is well and unhurried — not in the middle of a crisis. If you'd like help thinking it through sensibly and safely, I'm glad to sit down with you and your family. It's one of the kinder things you can set up for everyone's peace of mind.

PART 7

If It Happens to You

If something has already gone wrong, this part is your calm, step-by-step companion. There's no shame and no lecture here — just clear actions to limit the damage, report it, and get you safely back on your feet.

CHAPTER 70

First, Breathe — You're Going to Be Okay

If you're turning to this part because something has happened — you sent money, shared a code, clicked a bad link, or let someone into your computer — then first of all, stop and take a slow breath. You are going to be okay. A great deal can be undone or limited, especially if you act in the next little while, and I'll walk you through exactly what to do.

Three things to hold onto right now

- **You are not foolish.** These are professional criminals who fool sharp, careful people every day. Being targeted says nothing bad about you.
- **You are not alone.** This happens to enormous numbers of good people, and there is real help — your bank, the authorities, your family, and me.
- **Acting now helps.** The sooner you take the steps in this part, the more can often be stopped, frozen, or recovered.

FROM BILL

Call me, and we'll do it together

Please don't face this alone or sit with it in silence out of embarrassment. I have helped many good people through exactly this moment, calmly and without a word of judgment. Call me at (330) 200-8042 and we'll go through these steps together, one at a time, and get everything locked back down. That's what I'm here for.

How to use this part

The next chapters are organized by *what* happened — money sent, a password given, a computer accessed, your identity exposed. Go to the one that fits, do those steps, then read the chapter on reporting. Take them one at a time. You don't have to do everything in the next five minutes; you just have to start.

CHAPTER 71

The First Hour: Stop the Bleeding

Whatever happened, a few actions in the first hour matter most. Here's the short list to run through straight away; the later chapters add detail for each situation.

Right away, in order

1. **Stop all contact** with the scammer. Don't send another cent and don't believe that "one more payment" will fix or return anything — it won't.
2. **Call your bank or card company** if any money, card, or account details were involved — use the number on the back of your card. Tell them it's fraud.
3. **Change passwords** on anything that may be exposed — starting with your email, then your bank and anything sharing that password — and turn on two-factor.
4. **Disconnect the computer** from the internet if someone had remote access to it (unplug it or turn off the Wi-Fi), so they can't get back in.
5. **Write down what happened** while it's fresh — names, numbers, amounts, times. You'll need these for reports.

STAY SAFE

Don't let "one more payment" pull you back in

Scammers often promise that a further fee, tax, or payment will release your money, fix the problem, or undo the damage. It never does — it's just more theft. The moment you realize it's a scam, the single most protective thing you can do is **send nothing further** and break off contact completely.

CHAPTER 72

If You Sent Money

How you paid affects what can be done — but in every case, speed helps, so act as soon as you can. Here's what to do for each kind of payment.

If you paid by…	What to do
Bank transfer / wire	Call your bank immediately and say it's fraud. Fast action sometimes lets them recall or freeze a transfer before it clears.
Credit card	Call the card company, report fraud, and ask to dispute the charge. Credit cards offer strong protection and charges can often be reversed.
Debit card	Call your bank at once — protection is weaker than credit, so speed matters more. Ask them to stop the card and watch the account.
Gift cards	Call the card's company (number on the back) right away and report it; occasionally funds can still be frozen. Keep the card and receipt.
Money app (Zelle, Venmo, Cash App)	Report it in the app and to your bank immediately. These move fast and are hard to recover, but report anyway.
Cryptocurrency	Report to the exchange or app used and to the authorities. Crypto is very hard to recover, but reporting still helps investigators.

HEADS UP

Keep every scrap of evidence

Hold onto gift cards and their receipts, screenshots of messages, transaction numbers, emails, and any phone numbers. Don't throw anything away or delete the messages. This evidence helps your bank, the card companies, and investigators — and it's far easier to gather now than to reconstruct later.

CHAPTER 73

If You Gave a Password or Code

If you typed your password into a fake page, read a verification code to someone, or shared login details, the fix is to change the locks quickly. It's very doable — let's do it in order.

Change the locks, in order of importance

1. **Your email first** — it's the master key. Change its password and turn on two-factor right away, so crooks can't use it to reset your other accounts.
2. **Any account that shared that password** — change each one to its own new, strong password (now you see why reuse is dangerous).
3. **Your bank and financial accounts** — change passwords and turn on two-factor; call the bank if you're worried they got in.
4. **Check for sneaky changes** — look in each account's settings for a recovery email or phone number the crook may have added, and remove anything you don't recognize.

STAY SAFE

A code you shared may already be in use

If you read a two-factor code to someone, assume they tried to log in with it immediately. Change that account's password at once and check its security settings for anything the crook added. If you're locked out, use the account's "forgot password" recovery, or call me and we'll work through getting you back in.

FROM BILL

Locking things back down is very much fixable

Changing passwords across several accounts and checking each for tampering is methodical work, and it's exactly the sort of thing I help with often. If you're not sure you've caught everything, don't stew over it — call me and we'll go account by account until it's all secure and you can breathe easy again.

CHAPTER 74

If You Let Someone Into Your Computer

If a fake "tech support" person had you install a program and took control of your computer, don't panic — this is common and fixable. Here's how to shut them out and clean up.

The steps

1. **Disconnect from the internet** — unplug the network cable or turn off Wi-Fi — so they can't reach the computer anymore.
2. **Restart the computer.** This ends their active session.
3. **Remove the remote-control program** they had you install (things with names like AnyDesk, TeamViewer, or similar) — uninstall it, or have someone help you.
4. **Change your important passwords** from a *different*, trusted device (your phone), especially email and bank, in case they saw them.
5. **Call your bank** if you logged into banking while they were watching, and watch your accounts closely.
6. **Have the computer checked** by someone you trust to be sure nothing was left behind.

GOOD TO KNOW

They can't get back in once you've cut them off

A remote-support program only works while it's installed and the computer is online and running the session. Disconnect, restart, and remove the program, and the door is shut — they have no magic way back in. The remaining job is simply changing any passwords they might have seen and making sure the machine is clean.

FROM BILL

Let me check the computer properly

After a remote-access scam, it's worth having the computer looked over to be certain the bad program is gone and nothing was left behind. This is bread-and-butter work for me, and I do it without any fuss or judgment. Call (330) 200-8042 and we'll make sure your computer is truly yours again.

CHAPTER 75

If Your Identity May Be Stolen

If a crook got your Social Security number or enough details to open accounts in your name, a few powerful steps lock things down. These are the same protections from Part 6, now used with a bit more urgency.

Lock down your credit

1. **Freeze your credit** at all three bureaus — Equifax, Experian, and TransUnion — so no new accounts can be opened in your name. It's free.
2. Or at least place a free **fraud alert** (one call to one bureau sets it at all three), which tells lenders to verify it's really you before opening credit.
3. **Request your credit reports** at annualcreditreport.com and look for accounts or inquiries you don't recognize.

Then build your recovery plan

The U.S. government runs a free, friendly website just for this: **IdentityTheft.gov**. You tell it what happened, and it builds you a **personal step-by-step recovery plan** and even fills out some letters for you. It's genuinely helpful and worth using. Reach it by typing that address yourself.

WHAT THIS DOES FOR YOU

IdentityTheft.gov holds your hand

Identity theft can feel overwhelming — but you don't have to figure out the order of things alone. IdentityTheft.gov walks you through exactly what to do for your situation, in plain steps, and keeps track of your progress. Between that free tool, a credit freeze, and a phone call to me, you have everything you need to set this right.

CHAPTER 76

Where to Report It

Reporting a scam does real good: it helps investigators, it can trigger protections, and it helps warn and protect others. Here's where to report, depending on what happened. You needn't do all of them — pick the ones that fit.

What happened	Where to report
Any scam or fraud (FTC)	reportfraud.ftc.gov — the main place to report fraud of all kinds to the Federal Trade Commission.
Identity theft	IdentityTheft.gov — report and get a personal recovery plan.
Online crime (FBI)	ic3.gov — the FBI's Internet Crime Complaint Center, for online scams and larger losses.
Your bank / card company	The number on the back of your card — for anything involving your money or accounts.
Social Security scams	oig.ssa.gov — the Social Security Office of the Inspector General.
Medicare fraud	1-800-MEDICARE (1-800-633-4227), or report through medicare.gov.
Scam texts	Forward to 7726 (spells SPAM), free through your phone carrier.
Local police	For a report you can reference (useful for banks and insurers), and for in-person or local crimes.

TIP

Report even if you didn't lose money

You're worth listening to even if you caught the scam in time or lost nothing. Reporting a scam you spotted still helps the authorities track the crooks and warn others who might not be so quick. A few minutes at reportfraud.ftc.gov is a quiet good deed for your whole community.

CHAPTER 77

Beware the Recovery Scam

There's one more trap to warn you about, and it's a particularly heartless one: after you've been scammed, you may be targeted *again* by someone promising to get your money back. Knowing about it now means it can't catch you later.

How the recovery scam works

Weeks or months after a scam, you get a call, email, or message from a "recovery service," a "fraud investigator," a "lawyer," or even a fake "government agency" who says they can recover your lost money — for an upfront fee, or if you "verify" your bank details. It's the same crooks, or their friends, coming back for a second helping. There's no recovery; there's only another theft.

SCAM ALERT

Nobody legitimate charges an upfront fee to get your money back

Real help — your bank, the FTC, the police — never charges you an upfront fee to recover scammed money, and never asks for gift cards or your login to do it. Any "recovery service" that does is a scam. If someone contacts *you* promising to get your money back, treat it as another scam and don't pay a cent.

GOOD TO KNOW

Why victims get targeted twice

Once you've been scammed, your details may land on a "sucker list" that crooks trade — which is why the second wave comes. It's not bad luck or anything you did. Simply knowing the recovery scam exists makes you immune to it: real recovery never starts with a stranger calling you and asking for money.

CHAPTER 78

Recovering Your Peace of Mind

Being scammed takes more than money — it can shake your confidence and leave you embarrassed, angry, or afraid to use your devices at all. That part matters too, and it heals. Let's talk about it honestly.

Be gentle with yourself

The feelings are normal, and they pass. But please don't let them push you into hiding what happened or swearing off technology. The crook already took enough; don't let them also take your confidence or the connection and convenience your devices give you. You learned something, and you're more scam-proof now than you were before — that's a real silver lining.

Getting back on the horse, safely

- **Talk about it** — with family, a friend, or me. Saying it out loud drains away the shame and often turns up good practical help.
- **Tidy up your defenses** — this is a fine moment to set strong passwords, turn on two-factor, and freeze your credit, so you feel genuinely protected going forward.
- **Warn others** — your experience, shared kindly, may save a friend. That turns a bad day into something useful.

FROM BILL

No judgment, ever — and you're braver for facing it

If you've been through a scam, I want you to hear this plainly: it does not make you foolish, old, or any less capable. It makes you one of millions of good people targeted by professional criminals. Facing it, reporting it, and locking things down takes courage. I'm proud of you for it, and I'm always a phone call away at (330) 200-8042 — no lecture, just help.

PART 8

Safe Habits & When to Call Bill

We'll turn everything you've learned into a few easy habits that run on their own, a one-page cheat-sheet to keep by the phone, and an honest word about when to pick up the phone and call me.

CHAPTER 79

Building Safe Habits That Stick

You don't need to remember this whole book to stay safe. You need a handful of small habits that become second nature — so that staying safe takes no effort and no worry at all. Here are the ones that matter most, gathered in one place.

The daily habits

- **Slow down** when any message or call stirs up strong feeling or urgency. That pause is your whole defense.
- **Never send money, codes, passwords, or computer access** because of a call, text, email, or pop-up.
- **Reach companies your own way** — your bookmark, their app, or a number you look up — not through links or numbers a message gives you.
- **Let unknown calls go to voicemail**, and feel free to hang up on anyone at any time.
- **When in doubt, check with someone** — family, your bank, or me — before acting.

The habits that run themselves

- **Automatic updates** on your devices and apps.
- **Automatic backup** of your photos and files.
- **A password manager** (or a safe paper book) so every account has a strong, unique password.
- **Two-factor** turned on for email, bank, and your important accounts.
- **A credit freeze** quietly in place at all three bureaus.

WHAT THIS DOES FOR YOU

Set up once, protected for years

Notice that most of the strongest protections are things you set up *once* and then forget — updates, backup, two-factor, a credit freeze. A single afternoon of setup buys you years of quiet safety. If you do nothing else, do those once (I'm glad to help), and you'll be ahead of most people.

CHAPTER 80

Your Safety Checklist, Now and Then

Here's a gentle checklist you can run through — nothing urgent, just a tidy way to make sure your defenses are all in place and staying healthy. Tackle it a little at a time; there's no rush and no grade.

Set up once (do these, with help if you like)

The task	Done?
Strong, unique passwords on email, bank, and key accounts	[ ]
A password manager or a safe paper password book	[ ]
Two-factor turned on for email and bank	[ ]
Automatic updates turned on (phone, tablet, computer)	[ ]
Automatic backup turned on for photos and files	[ ]
Credit frozen at Equifax, Experian, and TransUnion	[ ]
Lock screen (PIN/face/fingerprint) on every device	[ ]
"Find My" turned on for phone and tablet	[ ]
Registered on the Do Not Call list; spam filtering on	[ ]

Check once in a while

- **Each month:** glance at your bank and card statements for anything you don't recognize.
- **Now and then:** check your credit reports at annualcreditreport.com.
- **Once a year:** confirm your backup is still running, and your recovery email and phone are current on key accounts.

TIP

A little at a time beats all at once

Don't feel you must do this whole list today. Tick off one or two items this week, a couple more next week. Each one you complete is real protection added. And any of them make a perfect thing to do together on a call or a visit if you'd rather not go it alone.

CHAPTER 81

Talking With Family About Scams

Scams thrive in silence, and they wither when families talk openly about them. A few easy conversations protect everyone — and they go both ways, because younger folks fall for scams too.

Easy ways to bring it up

- Share a scam *you* spotted — "I got the funniest fake toll text today" — which makes it normal to talk about, with no one on the spot.
- Agree on a **family code word** for emergency calls, so a fake "grandchild in trouble" call is caught at once.
- Make it a standing deal that **anyone can call anyone** to sanity-check a suspicious message, with no judgment, any hour.
- Decide, calmly, who the trusted helper is if someone's ever unwell, and where important account details are kept.

GOOD TO KNOW

Protection goes both ways

It's easy to think of this as the family protecting the elders, but scams hit every age — young people lose plenty to fake job offers, online shops, and crypto. Framing it as "let's all look out for each other" keeps it warm and mutual, and makes everyone more likely to speak up when something seems off.

CHAPTER 82

If You Think a Loved One Is Being Scammed

It's painful to watch someone you love being drawn into a scam — a new online sweetheart, a "great investment," a stream of gift-card purchases. How you step in makes all the difference, because shame and argument tend to push people deeper in.

What helps

- **Lead with care, not blame.** "I love you and I'm worried" opens a door; "How could you fall for that?" slams it shut.
- **Ask gentle questions** and really listen — have they met this person? Why the gift cards? — rather than lecturing.
- **Share the pattern**, not a put-down: secrecy, urgency, and requests for untraceable money are the universal signs.
- **Offer to help check** together — call the bank, look up the company, slow things down as a team.

If they're caught up and can't see it

Deep scams — especially romance and investment ones — can have a powerful emotional hold, and the person may defend the scammer. Stay patient and keep the relationship warm; pushing too hard can isolate them further. Enlist others they trust, involve the bank (who can sometimes flag or slow transfers), and reach out to the resources in this book. And remember you can always call me for a steady, judgment-free hand.

FROM BILL

I'm glad to be the neutral voice

Sometimes a loved one will hear from an outside, patient professional what they can't quite hear from family. If someone you love is in the grip of a scam and you don't know how to reach them, call me at (330) 200-8042. I'll help gently, without judgment, and often a calm third party is exactly what breaks the spell.

CHAPTER 83

Staying Calm as the Scams Change

Scams will keep evolving — new costumes, new technology, new headlines. That's exactly why this book taught you the *pattern* rather than a list to memorize. Let's close that loop so you feel ready for whatever comes next.

A quick word on new tricks

You'll hear about new wrinkles — scammers using recordings to fake a loved one's voice, or fake video, or ever-slicker fake websites. The technology gets fancier, but look closely and the machine underneath is always the same: **strong feeling, a rush, and a push to send something that can't be undone.** A faked voice still can't survive you hanging up and calling your grandchild back on their real number.

STAY SAFE

The pattern never goes out of date

No matter how new or clever a scam sounds, run it through the same three questions: Is someone stirring up strong feeling? Am I being rushed? Are they asking me to send money, a code, or access? If yes, slow down and check — and you've beaten it, whatever costume it was wearing. That test will still work years from now.

Where to keep learning, calmly

- The FTC's consumer site (consumer.ftc.gov) posts plain-English alerts about current scams.
- Your bank and AARP share timely warnings written for everyday folks.
- And me — I keep up with what's going around Portage County, and I'm always glad to tell you what I'm seeing.

CHAPTER 84

A Plain-English Safety Glossary

The safety world is full of jargon that makes simple ideas sound scary. Here's a plain dictionary of the words you'll meet, so none of them can intimidate you. Keep it handy; soon you won't need it.

Word	What it means
Scam / fraud	A trick designed to take your money or information.
Phishing	A fake email trying to "fish" your password or details out of you.
Smishing	The same trick by text message (SMS).
Spoofing	Faking the name or number that shows on your phone or in an email.
Malware / virus	Harmful software that sneaks onto a device, usually by being installed.
Ransomware	Malware that locks your files and demands payment — beaten by having a backup.
Two-factor (2FA)	A second step at login — a code or tap — on top of your password.
Password manager	A locked "safe" app that remembers all your passwords for you.
Passkey	A newer password replacement that can't be stolen or phished.
Encryption	Scrambling data so only the right people can read it (the padlock).
https / padlock	The sign that your connection to a website is private.
Data broker	A company that collects and sells people's personal details.
Credit freeze	A free lock on your credit file so no new accounts can be opened in your name.
Fraud alert	A free flag telling lenders to double-check it's really you.
Identity theft	A crook using your details to pose as you — open accounts, claim benefits.
Remote access	Letting someone control your computer from afar — only ever for people you trust.
Cookie	A small note a website leaves to remember you; mostly harmless.
VPN	A tool that adds privacy to your internet connection (optional, not essential).

CHAPTER 85

Your One-Page Scam Cheat-Sheet

Tear this page out, or fold its corner, and keep it by the phone or the computer. If you remember nothing else, this one page will carry you safely through almost anything.

The one rule

Slow down. Never send money, gift cards, codes, passwords, or computer access because of a call, text, email, or pop-up — no matter who it claims to be. Hang up or close it, and check with a real person first.

Dead giveaways it's a scam

If you see or hear this…	It's a scam
"Buy gift cards and read me the numbers"	Always — no exceptions
"Act now," "don't hang up," "tell no one"	Urgency + secrecy = scam
"Move your money to keep it safe"	Your bank never says this
"Your SSN is suspended" / "warrant for arrest"	Government-impersonation scam
A pop-up or call about a computer virus	Tech-support scam — hang up / restart
"You've won" but must pay a fee first	Prize scam
"Guaranteed" big investment returns	Investment/crypto scam
A link in a text for a package, toll, or account	Smishing — don't tap; go to the source

What to do in the moment

Situation	Do this
Pressured on the phone	"I'll call back on a number I look up." Hang up.
Worrying email or text	Don't click. Open the account your own way and check.
Scary pop-up on screen	Don't call the number. Close it or restart the device.
Not sure if it's real	Stop. Check with family, the bank, or Bill before acting.
Already sent money/codes	Call your bank now; see Part 7; call Bill — no shame.

Numbers worth keeping

For…	Reach
Report any fraud	reportfraud.ftc.gov
Identity theft help	IdentityTheft.gov

For…	Reach
Medicare	1-800-MEDICARE (1-800-633-4227)
Report scam texts	Forward to 7726
Bill's Home Tech	(330) 200-8042

CHAPTER 86

When to Call Bill

I wrote this book so you could stay safe online yourself, at your own pace, with confidence. And you can. But part of doing things well is knowing when to hand a worry to someone who does this every day — so you can get on with enjoying life instead of fretting. Here's my honest take on when to pick up the phone.

Good reasons to call

- You got a message, call, or offer that feels off and you'd like a **second opinion** before you do anything — always a good call, never a bother.
- You think you may have been **scammed**, or let someone into your computer, and you want a calm hand to help you lock things down.
- You'd like to **set up your protections properly** — passwords, two-factor, backups, a credit freeze — together, once, so you can stop worrying.
- A pop-up, a locked-up computer, or a suspicious program has you stuck.
- You simply want to **learn** — how to spot the fakes, use a password manager, shop and bank safely — with a patient person beside you.

What working with me is like

I'm Bill, and I run **Bill's Home Tech** right here in Portage County, Ohio. I've spent **30+ years** helping people feel at home and safe with their technology, and I treat every call the way I'd want my own parents treated: patiently, in plain English, with no rushing, no jargon, and never, ever any eye-rolling or judgment. There is no such thing as a silly question with me — and there is certainly no shame in having been targeted by a scam.

How to reach me	
Call or text	(330) 200-8042
Book online	billshometech.com/book
Where I serve	Portage County, Ohio and nearby
What it costs	Fair, honest, and told to you up front — no surprises

FROM BILL

You're never a bother — that's the whole job

Some folks hesitate to call because they don't want to be a nuisance, or they're embarrassed about a scam. Please don't feel that way. Helping you is not an interruption to my work — it *is* my work, and it's work I love. Whether it's a five-minute "is this real?" question or helping you recover from something bigger, I'm glad to help. That's what I'm here for.

GOOD TO KNOW

If you reach my website, you may meet Sophie

When you visit billshometech.com, you might be greeted by **Sophie**, my friendly assistant on the site. She can answer quick questions and help you book a time with me. She's there to make reaching me easier — but a real person (me) always does the actual help, and I'll never ask you for a password or a payment by gift card.

Thank you for letting me be your guide to staying safe online. You don't need to be afraid of your phone, your computer, or the internet — you need to be unhurried, and now you are. Take your time, trust that steady judgment you've built over a lifetime, and remember: when in doubt, slow down and make a call. You're never stuck alone. I'm proud of you for learning all this.

— Bill