BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

Spotting & Avoiding Scams

Phone, email, text, and pop-up scams —
how to see them coming, explained in plain English

A plain-English guide to staying a step ahead

Knowledge is your armor — and you can't be fooled twice

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

Current scam tactics · facts current November 2026

What's Inside

This is your scam-safety manual — maybe the most important one in this whole series. In plain English, it shows you exactly how the scams of today work: the phone calls, the emails and texts, the alarming pop-ups, and the too-good-to-be-true offers. Once you can see the few tricks they all rely on, they lose their power over you. This book isn't here to frighten you — it's here to make you confident and hard to fool. Read it in any order, and keep it close.

Part 1 — Understanding Scams

1 A Note from Bill
2 What a Scam Actually Is
3 Why Scammers Target Older Adults
4 The Feelings They Exploit
5 The Universal Red Flags
6 Bill's Golden Rules
6a Scams Are Old — Only the Costumes Change
6b Why Smart People Fall for Scams
6c The One-Minute Scam Check

Part 2 — The Machinery of a Scam

7 The Pressure Playbook
8 Why They Demand Gift Cards and Wires
9 How They Keep You From Checking
10 Spoofing: When Caller ID and Addresses Lie
11 The “Money Mule” and Other Ways They Use You
11a QR Code Scams
11b Text Message Scams (“Smishing”)
11c Robocalls and the One-Ring Trick
11d Payment Apps: Zelle, Venmo, and Cash App
11e Cryptocurrency, Explained Simply

Part 3 — Phone Scams

12 How to Handle Any Suspicious Call
13 The Grandparent / Family Emergency Scam
14 The “Tech Support” Call
15 Government Impersonation: IRS, Social Security, Police
16 The Bank “Fraud Department” Call
16a The Jury Duty / Warrant Scam
16b Utility and Service Shut-Off Scams
16c Voicemail, Callback, and “Survey” Traps

16d Fake Debt Collectors
16e The “Your Car's Warranty” and Other Nuisance Calls

Part 4 — Email & Text Scams

17 Phishing: The Art of the Fake Message
18 The Red Flags in a Message
19 The Fake Delivery Notice
20 “Your Account Has a Problem”
21 Lottery, Prize, and “Free Money” Scams
21a Dangerous Attachments
21b Unsubscribe Traps and Reply Bait
21c Business and Invoice Email Scams
21d How to Check Who Really Sent an Email
21e Spam vs. Scam: Knowing the Difference

Part 5 — Computer & Pop-Up Scams

22 The Scary Pop-Up
23 What to Do When a Pop-Up Strikes
24 If You Let Someone Into Your Computer
25 Fake Antivirus and “Tune-Up” Software
25a The Fake “Support Number” You Find by Searching
25b Fake Updates and “Your Device Is Infected” Apps
25c Public Wi-Fi and Charging Cautions
25d Fake Websites and Login Pages
25e Keeping Your Web Browsing Safe

Part 6 — Online Scams

26 Romance Scams
27 Investment and Cryptocurrency Scams
28 Online Shopping and Marketplace Scams
29 Charity, Medicare, and Other Impersonations
29a Social Media Scams
29b Fake Jobs and Work-from-Home Scams
29c Too-Good Deals: Pets, Rentals, and Timeshares
29d Sweepstakes, Lotteries, and “You're Pre-Approved”
29e Giving to Charity Safely

Part 7 — Protecting Yourself & Recovering

30 Your Everyday Defenses
31 Locking Down Your Accounts and Credit
32 If You Think You've Been Scammed
33 Beware the “Recovery” Scam

34 Helping a Loved One Stay Safe
34a Watching Your Accounts and Identity
34b What Scammers Do With Your Information
34c Scam-Proofing Your Phone and Devices
34d The Emotional Side of Being Scammed
34e Talking With Grandchildren and Family About Scams

Part 8 — When to Call Bill & Your Cheat-Sheet

35 When to Call Bill
36 Your Scam-Safety Cheat-Sheet

PART 1

Understanding Scams

What a scam really is, why decent and intelligent people fall for them, the feelings scammers exploit, and the small set of warning signs that appear in nearly every one. Start here.

CHAPTER 1

A Note from Bill

Hello, and welcome. Whoever is holding this book — this is for **you**, and I want to start by saying something plainly: if you've ever been fooled by a scam, or worry you might be, you are not foolish, not gullible, and not alone. The people who run these schemes are professional, organized, and relentless, and they fool sharp, careful, successful people every single day. There is no shame here — only knowledge to be gained.

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 way I'd sit beside you at your kitchen table: patiently, in plain English, with no lecturing. My goal is simple — to hand you the same understanding the scammers hope you never get, so their tricks stop working on you.

Why I care so much about this one

Of all the house calls I make, the ones that stay with me are the people who've lost their savings to a scam — good people, caught in a frightening, fast-moving moment. Almost every one of those losses could have been prevented by knowing a few things in advance. That's what this book gives you: not fear, but the quiet confidence of someone who knows the tricks and can't be rushed into a mistake.

WHAT THIS DOES FOR YOU

Knowledge is the one thing scammers can't take

Scammers rely on surprise and on you not knowing how their game works. Once you *do* know — once you can name the trick as it's happening — the spell breaks. This whole book is really about one gift: making you the person who sees it coming, stays calm, and hangs up. That person almost never gets scammed.

And I'm only a phone call away

The single best habit in this entire book is this: **when something feels off, stop and check with someone you trust before you act.** I would far rather get a call about a message that turns out to be nothing than a call after money is gone. Call me at **(330) 200-8042** any time, about anything that gives you pause. No judgment, no silly questions — ever.

So let's pull back the curtain on how these schemes work. By the end, you'll see them coming a mile off.

— Bill

CHAPTER 2

What a Scam Actually Is

Let's start with a clear definition. A **scam** is a deliberate trick designed to get you to hand over money, personal information, or access to your accounts — usually by pretending to be someone or something you trust, and by rushing you so you don't have time to think clearly.

Two things every scam needs

- **A disguise.** The scammer pretends to be someone trustworthy — your bank, the government, a tech company, a charity, even a grandchild. The disguise is what gets your guard down.
- **A push.** They create pressure — urgency, fear, or excitement — so you act *before* you think. The push is what gets your money out the door.

Strip away the particulars — the phone call, the email, the pop-up — and almost every scam is just those two things: a mask and a shove. Learn to spot the mask slipping and the shove coming, and you've learned to spot nearly any scam, no matter how it's dressed.

GOOD TO KNOW

Scammers are in the business of emotions, not technology

It's tempting to think scams are a technology problem, but they're really an *emotion* problem. The scammer's true target isn't your computer — it's your feelings: your fear of trouble, your love for family, your hope of a windfall. The technology is just the delivery van. That's why the defenses in this book are mostly about slowing down and thinking, not about gadgets.

CHAPTER 3

Why Scammers Target Older Adults

It's an uncomfortable truth, but an important one to understand: scammers deliberately aim at older adults. Knowing *why* isn't meant to alarm you — it's meant to help you see exactly where you're a target, so you can be ready.

The honest reasons

- **A lifetime of savings.** Retirees often have more money set aside than younger people — and scammers follow the money.
- **Trust and politeness.** Many older folks were raised to be courteous and to trust authority, which scammers exploit by posing as officials.
- **Less familiarity with the newest tricks.** The schemes change fast; it's not about intelligence, just exposure.
- **Sometimes, isolation.** Someone who lives alone may have no one in the room to say "wait, this sounds wrong."

FROM BILL

Being targeted is not the same as being foolish

I want to be very clear, because it matters: being *targeted* says nothing about your intelligence — it says the scammers did their math. The sharpest, most accomplished people I know have been nearly caught. This book simply levels the field: it gives you the awareness the scammers are betting you don't have. Knowing you're a target is the first step to being a hard one.

Turning the tables

Here's the empowering flip side. The very fact that scammers rely on surprise means that a prepared person — someone who's read a book like this — is remarkably safe. You can't be ambushed by a trick you already recognize. By the time you finish these pages, you'll be exactly the kind of person scammers hate: calm, informed, and impossible to rush.

CHAPTER 4

The Feelings They Exploit

Every scam works by stirring up a strong feeling and then using that feeling to hurry you. If you learn to notice the *feeling* itself as a warning sign, you can catch almost any scam in the act — before the details even matter.

The four feelings to watch for

The feeling	How it's used against you
Fear	“Your account is compromised!” “You owe back taxes!” “You'll be arrested!” Fear makes you obey.
Urgency	“Act in the next hour or else.” Urgency stops you from pausing to check.
Greed / hope	“You've won!” “Double your money!” Excitement switches off caution.
Love / sympathy	“Grandma, I'm in trouble, please help.” Love makes you act without thinking.

SCAM ALERT

The feeling IS the warning sign

Here is one of the most powerful ideas in this book: **a sudden rush of fear, urgency, excitement, or alarm — combined with pressure to act right now — is itself the red flag.** You don't even need to figure out the specific trick. The moment a call, message, or pop-up makes you feel that surge and wants you to hurry, treat the feeling as the alarm bell it is. Stop, breathe, and check.

Why slowing down beats everything

Scammers need you to act *in the moment*, while the feeling is hot, because they know that given five minutes and one calm conversation, the trick falls apart. That's their one great weakness — and your one great defense. Almost nothing legitimate in life requires you to act within the hour without checking. When someone insists you must, that insistence is the scam showing its hand.

CHAPTER 5

The Universal Red Flags

Although scams come in endless costumes, the warning signs are remarkably few and remarkably consistent. If you memorize just this one chapter, you'll be able to spot the great majority of scams. These are the signals that should make you stop every time.

The red flags, all in one place

- **Pressure to act immediately** — “right now,” “or else,” a countdown, a threat.
- **A request for secrecy** — “don't tell anyone,” “keep this between us.”
- **A demand for unusual payment** — gift cards, wire transfer, cryptocurrency, payment apps, cash by courier.
- **A request for personal information or passwords** — Social Security number, bank details, login codes.
- **Contact you didn't initiate** — an out-of-the-blue call, email, or text about a problem or prize.
- **Too good to be true** — a prize you didn't enter, a return that's too high, a romance that moves too fast.
- **They won't let you verify independently** — they discourage you from hanging up and calling the real number.

STAY SAFE

Any ONE of these is reason enough to stop

You don't need to see all seven — **any single one of these red flags is reason enough to stop, hang up, and check independently.** Real companies and real agencies don't rush you, don't swear you to secrecy, don't demand gift cards, and don't mind one bit if you call them back on a number you look up yourself. When even one flag is flying, trust it.

Keep this list where you can see it

This is the heart of the whole book, so I'd encourage you to copy these red flags onto a card and keep it by the phone and the computer. In the heat of a scammer's call, a glance at that card can be the thing that saves you. There's a ready-made version in the cheat-sheet at the very back.

CHAPTER 6

Bill's Golden Rules

If the red flags are how you *spot* a scam, these golden rules are how you *defeat* one. They're simple, they're memorable, and together they'll carry you safely through almost anything a scammer tries.

The rules that keep you safe

1. **Slow down.** No honest matter requires you to act within minutes. Pressure to hurry is itself the warning.
2. **Hang up and verify.** Never trust a caller's identity. Hang up and call back on a number *you* look up — on your card, your bill, the real website.
3. **Never pay with gift cards, wire, or crypto** to someone who contacted you. These are scammer favorites because they can't be reversed.
4. **Never give passwords, codes, or remote access** to anyone who contacts you, for any reason.
5. **Talk to someone you trust** before acting on anything urgent or money-related. Saying it out loud breaks the spell.
6. **When in doubt, do nothing yet.** Doing nothing for an hour has never cost anyone their savings. Acting in haste has.

TIP

“I never do business with anyone who calls me.”

Here's a single sentence that can replace this whole book in a pinch: **“I don't give information or money to anyone who contacts me first — I always hang up and reach out myself.”** Say it, mean it, and stick to it without exception, and you'll sidestep the overwhelming majority of scams. It's perfectly polite, and it's bulletproof.

FROM BILL

You're allowed to be “rude” to a scammer

Many good people get caught partly because they were raised not to be impolite — they don't want to hang up on someone. Let me free you from that right now: **you owe a scammer nothing.** Hanging up mid-sentence on a suspicious caller isn't rude; it's smart. A real person will understand you calling back to verify. A scammer is counting on your manners. Hang up with a clear conscience.

CHAPTER 6a

Scams Are Old — Only the Costumes Change

It can feel as though scams are a frightening new product of the internet age. They aren't. Con artists have worked the same handful of tricks for centuries — the fake official, the sudden windfall, the urgent emergency. Only the delivery has changed, from a knock at the door to a ring of the phone to a ping on the screen.

Why this is good news

Here's why that matters: because the underlying tricks are old and few, you don't have to learn a thousand new scams. Learn the *handful of timeless moves* — false authority, urgency, secrecy, a demand for untraceable payment — and you'll recognize them in whatever modern costume they wear, including scams that haven't been invented yet. The technology keeps changing; human nature, and the con, do not.

GOOD TO KNOW

New technology, same old trick

When you hear about a frightening “new” scam — AI voices, crypto, QR codes — look past the technology to the trick underneath. Nearly always it's one of the classics: pretend to be someone trusted, stir up a strong feeling, and rush you into paying. Spot the old bones inside the new costume, and the “new” scam holds no surprises.

CHAPTER 6b

Why Smart People Fall for Scams

If you've ever thought “I'd never fall for that,” I gently want to challenge it — not to worry you, but to protect you. The belief that only foolish people get scammed is itself dangerous, because it makes you lower your guard and feel too ashamed to ask for help if something happens.

The real reasons good people get caught

- **They were caught at a bad moment** — tired, distracted, grieving, or genuinely expecting a call or package.
- **The scam was professional** — polished, researched, and emotionally expert.
- **Strong emotion overrode judgment** — fear or love makes anyone act against their better sense.
- **It happened fast** — the whole point of the rush is to beat your common sense to the punch.

FROM BILL

“I'd never fall for that” is exactly what scammers hope you think

Overconfidence is a scammer's friend. The people who stay safest aren't those who feel immune — they're those who respect how good these crooks are and stay humble and careful. So rather than “I'd never fall for that,” try “anyone can be caught, so I'll always slow down and check.” That humble habit is far stronger armor than confidence ever was.

CHAPTER 6c

The One-Minute Scam Check

Let's distill everything into a tool you can run in your head in under a minute, any time something feels off. Four quick questions, and most scams reveal themselves.

Ask yourself these four questions

1. **Did they contact me, or did I reach out?** If they contacted me out of the blue, be wary.
2. **Are they rushing me or scaring me?** Urgency and fear are the scammer's tools.
3. **Are they asking for money, secrets, or access?** — gift cards, passwords, remote control, personal details.
4. **Can I hang up and verify this myself?** If they resist that, it's almost certainly a scam.

TIP

Four questions that fit on a sticky note

Write these four questions on a note by your phone. When any call or message makes you uneasy, run through them. If the answers are “they contacted me, they're rushing me, they want money or secrets, and they don't want me to check” — you have your answer. Hang up. This little mental checklist is the whole book boiled down to something you can use in the heat of the moment.

WHAT THIS DOES FOR YOU

A calm minute defeats a practiced criminal

It's a remarkable thing: a professional scammer, with all their scripts and pressure, is undone by one ordinary person taking a calm minute to ask four simple questions. That minute is your superpower. They have everything riding on you *not* taking it — so taking it, every time, is how you win.

PART 2

The Machinery of a Scam

A look under the hood at the tools every scammer uses — the pressure tactics, the demand for untraceable payment, and the ways they try to keep you from checking with anyone.

CHAPTER 7

The Pressure Playbook

Scammers follow a surprisingly consistent script, because it works. Once you can recognize the moves — like knowing a magician's tricks — the performance stops fooling you. Here's the playbook they run again and again.

The classic sequence

1. **Grab your attention with alarm or excitement** — a problem, a threat, or a prize.
2. **Establish false authority** — “This is the IRS,” “I'm from Microsoft security,” “I'm Officer Smith.”
3. **Create urgency** — “You must act now or the police are coming / the account closes / the prize expires.”
4. **Isolate you** — “Don't hang up,” “don't tell your family,” “keep me on the line.”
5. **Extract money or information** — gift cards, a wire, your passwords, remote access to your computer.

GOOD TO KNOW

Recognizing the script is half the battle

The moment you notice a call or message marching through these steps — alarm, authority, urgency, isolation, the ask — you can name it: “this is the scam playbook.” That recognition alone pops the bubble. Real institutions simply don't operate this way; they don't threaten, rush, and swear you to secrecy. The script itself is the confession.

CHAPTER 8

Why They Demand Gift Cards and Wires

If you remember only one concrete fact from this book, make it this one, because it catches an enormous share of scams: **the payment method a scammer demands is a dead giveaway.** Let's understand why.

The scammer's favorite payments

Payment they demand	Why scammers love it
Gift cards	You buy cards at a store and read them the numbers. Untraceable, irreversible. A screaming red flag.
Wire transfer	Money sent by Western Union / MoneyGram or bank wire — gone instantly, almost never recoverable.
Cryptocurrency	Bitcoin and the like, often via a "crypto ATM." Anonymous and irreversible.
Payment apps to strangers	Zelle, Cash App, Venmo sent to someone you don't know — like handing over cash.
Cash by courier / mail	Someone sends a driver to collect cash or a package. Always a scam.

SCAM ALERT

No real institution is ever paid in gift cards

Burn this in: **the IRS, Social Security, your bank, the electric company, Amazon, Apple, Microsoft, the police — none of them is ever, ever paid in gift cards, wire transfers, or cryptocurrency.** There are zero exceptions. The instant anyone asks you to pay a bill, fine, fee, or debt this way, you are certainly talking to a scammer. Stop immediately and call someone you trust.

Why these methods, really

All of these share one feature: **once the money is gone, it can't be clawed back.** A credit card charge can be disputed; a check can be stopped; but gift-card codes, wires, and crypto vanish the moment they're handed over. Scammers insist on them precisely *because* there's no undo button. The payment method is the scam's weakest disguise and your easiest tell.

CHAPTER 9

How They Keep You From Checking

A scammer's greatest enemy is a second opinion — a moment where you hang up and call the real company, or where a family member hears what's happening and says “that's a scam.” So a huge part of their craft is keeping you isolated and on the hook. Knowing these tactics makes them backfire.

The isolation tricks

- **“Stay on the line”** — they keep you on the phone, sometimes for hours, even while you drive to buy gift cards, so no one can intervene.
- **“Don't tell anyone”** — they frame secrecy as part of an “investigation,” or say your family is involved, or that you'll be in trouble if you talk.
- **“Your bank / family can't be trusted”** — they try to turn you against the very people who'd protect you.
- **Discouraging you from calling back** — “there's no time,” or they give you a fake “direct number” that just rings them again.

STAY SAFE

Secrecy is a scam tactic — always break it

No legitimate bank, agency, or company will *ever* tell you to keep a matter secret from your family, or forbid you to hang up and call them back. That demand for secrecy is one of the surest signs of a scam in the entire book. The correct response to “don't tell anyone” is to immediately tell someone. Secrecy protects the scammer, never you.

The power of one phone call

This is why Bill's golden rule — *talk to someone you trust before acting* — is so mighty. The simple act of describing the situation out loud to another person almost always makes a scam obvious, because you hear how strange it sounds. Scammers know this, which is exactly why they work so hard to stop you doing it. So make that call. It's the single most protective thing you can do.

CHAPTER 10

Spoofing: When Caller ID and Addresses Lie

Here's a fact that surprises many people and that scammers rely on heavily: **the name and number you see on a caller ID, and the name on an email, can be faked.** This is called “spoofing,” and understanding it removes one of the scammer's best disguises.

What spoofing means

- **Phone spoofing:** a scammer can make your phone show “IRS,” “Social Security,” your bank's name, or even a local number — none of it real.
- **Email spoofing:** the sender name can say “Amazon” or “Your Bank” while the real address behind it is something else entirely.
- **Text spoofing:** a text can appear to come from a short “official” number or even thread into real messages.

HEADS UP

A familiar name on your screen proves nothing

Because caller ID and sender names can be faked, **seeing a trusted name is not proof of anything.** This is crucial: never trust that a call is really from your bank just because the screen says so. The only way to know who you're truly dealing with is to *hang up and call back on a number you look up yourself.* The screen can lie; a number you dialed yourself cannot.

The defense is always the same

You don't need to become a technology expert to beat spoofing. The defense is the same humble habit that beats nearly everything in this book: don't trust incoming contact, and verify independently. Hang up, look up the real number, and call it. If the “bank” on your screen was real, you'll reach them; if it was a scammer, you've just walked away untouched.

CHAPTER 11

The “Money Mule” and Other Ways They Use You

Some scams don't just take your money — they try to use you to move *other* people's stolen money, which can land you in real legal trouble without your realizing it. This is worth understanding so you're never unwittingly drawn in.

How it works

A scammer (sometimes posing as a romantic interest, an employer, or a “government agent”) asks you to **receive money and then forward it on** — depositing a check and wiring part of it elsewhere, or accepting funds in your account and passing them along. The money is stolen, the check is fake, and you can be left owing the bank and facing questions from authorities. The scammer has used you as a “mule.”

STAY SAFE

Never receive and forward money for someone you don't know

A simple, firm rule: **never agree to accept money and send it on** for anyone you haven't known and trusted for years in person — no matter the story, the romance, or the “job.” Legitimate work and real relationships don't ask this. If someone wants to route money through your account, it's a scam that can make you an unwitting accomplice. Decline, and tell your bank.

Fake checks and overpayments

A close cousin is the **fake check** scam: you're sent a check for more than expected and asked to “refund the difference,” or to deposit a check and buy gift cards with part of it. The check looks real and your bank may even show the funds at first — but days later it bounces, and you're on the hook for everything you sent. Never send money based on a check that just arrived, however official it looks.

GOOD TO KNOW

A deposited check isn't really “cleared” for days

Banks often make funds from a check *available* within a day or two, but that is not the same as the check having truly *cleared* — which can take a week or more. Scammers exploit exactly that gap. So never spend or forward money from a check until your bank confirms it has genuinely cleared. When in doubt, ask a teller directly, “Has this actually cleared?”

CHAPTER 11a

QR Code Scams

A **QR code** is one of those little square checkerboard patterns you scan with your phone's camera to open a website. They're handy and everywhere now — which is exactly why scammers have started using them to send people to fake pages.

How the scam works

- A scammer puts a QR code on a **fake parking meter sticker, a phony parcel notice, or in an email**, so scanning it opens a counterfeit payment or login page.
- Because you can't read a QR code with your eyes, you can't tell where it leads until you've scanned it — a perfect disguise.
- The fake page then asks for your card details or password, just like any phishing site.

HEADS UP

Treat a QR code like a link from a stranger

A QR code is just a link you can't read in advance, so give it the same caution you'd give any link: be very wary of scanning one from an unexpected email, a sticker in public, or a mailed “notice.” After scanning, *check the web address* that opens before typing anything — if it's not the genuine company's site, back out. When in doubt, don't scan; reach the company the usual way instead.

CHAPTER 11b

Text Message Scams (“Smishing”)

Scam texts — nicknamed **“smishing”** (SMS + phishing) — have exploded, because texts feel personal and get read quickly. They use every trick of email phishing, squeezed into a short message with a tempting link.

Common scam texts

The text	What it really is
“Your package couldn't be delivered…”	Fake carrier notice with a link. (See Chapter 19.)
“Your bank account is locked…”	Fake bank alert to steal your login.
“Hi, is this [name]? :)” from a stranger	A “wrong number” opener that leads to a romance or investment scam.
“You have a toll / ticket to pay…”	Fake fee notice with a payment link.
“IRS / government benefit…”	Impersonation to harvest your details.

STAY SAFE

Don't tap links in texts — and don't reply to strange ones

The rule for texts is the same as for email: **don't tap a link in an unexpected text,** and don't reply to a mysterious “wrong number” that turns chatty. Replying — even “you have the wrong number” — tells a scammer your number is live and reaches a real person, inviting more. For anything that might be real (a package, a bank alert), check through the official app or a number you look up. Then simply delete the text.

Report and block

You can forward spam texts to **7726** (which spells “SPAM”) to report them to your phone carrier, then block and delete the sender. Your phone also has a setting to filter messages from unknown numbers into a separate list. These quietly reduce the flood — ask me and we'll switch them on together.

CHAPTER 11c

Robocalls and the One-Ring Trick

Robocalls — automated calls that play a recording — are the delivery truck for countless phone scams, dialing millions of numbers cheaply. Understanding them helps you shrug them off.

What to know about robocalls

- **Pressing a button to "stop calls" or "speak to someone" usually makes it worse** — it confirms a live person and invites more. Just hang up.
- **The "one-ring" scam** calls and hangs up, hoping you'll call back a number that charges you high fees. Don't call back numbers you don't recognize.
- **Your caller ID may show a local number** ("neighbor spoofing") to get you to answer. A familiar area code proves nothing.

TIP

Let unknown numbers go to voicemail — every time

The simplest robocall defense costs you nothing: don't answer numbers you don't recognize. Real callers leave a message; robocallers and scammers rarely do. You can return any genuine call afterward, on your own terms, having looked up the number. Silence really is golden here — every unanswered scam call is a scam that never got started.

GOOD TO KNOW

"Silence Unknown Callers" can give you peace

Both iPhone and Android have a setting — often called **Silence Unknown Callers** — that sends calls from numbers not in your contacts straight to voicemail without ringing. If robocalls are driving you to distraction, this can be a blessing (just add the people you want to hear from to your contacts first). Ask me and we'll turn it on if you'd like.

CHAPTER 11d

Payment Apps: Zelle, Venmo, and Cash App

Payment apps — Zelle, Venmo, Cash App, PayPal — let you send money from your phone in seconds. They're convenient for paying family and friends, but that speed is exactly why scammers push them: money sent this way is usually **gone instantly and can't be reversed**, like handing over cash.

Using them safely

- **Only send to people you know and trust.** Treat it like cash from your wallet.
- **Double-check the name and number** before sending — a typo sends money to a stranger who may not return it.
- **Never send to someone who contacted you** about a prize, bill, refund, or emergency.
- **Ignore "accidental payment" scams** — if a stranger "accidentally" sends you money and asks you to send it back, stop; it's a trick involving stolen funds.

SCAM ALERT

These apps are like cash — no refunds for scams

The crucial thing to understand: unlike a credit card, money sent through Zelle, Venmo, or Cash App generally **cannot be recovered** if you're scammed — there's no dispute process like a card has. That's precisely why scammers insist on them. So use them only to pay people you personally know, and never to pay a stranger, a "company," or anyone who contacted you. When in doubt, use a credit card instead.

CHAPTER 11e

Cryptocurrency, Explained Simply

You hear “cryptocurrency” and “Bitcoin” in scam warnings constantly, so let's demystify it. You don't need to understand the technology — just enough to know why scammers love it and to steer clear.

What it is, in plain terms

Cryptocurrency is a kind of digital money that exists only online, with no bank behind it. Its defining feature, for our purposes, is that payments are **anonymous and irreversible** — once you send it, it's gone, with no company to call and no way to reverse it. Some people invest in it legitimately; but for a scammer, it's the perfect way to collect money that can never be traced or clawed back.

SCAM ALERT

“Pay with Bitcoin” or a “crypto ATM” is a giant red flag

A particularly common trap: a scammer (posing as the government, tech support, or a sweetheart) directs you to take cash to a **“crypto ATM”** — a machine in a store — and convert it to cryptocurrency sent to their “wallet.” **No legitimate agency, company, or person you've just met will ever ask you to pay in cryptocurrency.** If anyone directs you to a crypto ATM, it is a scam, 100% of the time. Walk away.

FROM BILL

Curious about crypto? Learn before you ever buy

If cryptocurrency genuinely interests you as an investment, that's your choice — but please learn about it from independent, trustworthy sources first, and never on the urging of someone who contacted you or promised big returns. I'm glad to talk through the *scam-safety* side with you (I'm not a financial advisor). The one firm rule: never send crypto to anyone who reached out to you. Call (330) 200-8042 if you'd like to talk it through.

PART 3

Phone Scams

The telephone is still the scammer's favorite tool. Here are the calls you'll get — the fake grandchild, the “tech support” warning, the IRS threat, the bank “fraud department” — and exactly how to handle each.

CHAPTER 12

How to Handle Any Suspicious Call

Before we go through the specific phone scams, here's the master response that works for *all* of them. Learn this one routine and you're protected against every phone scam in this part, even brand-new ones you've never heard of.

The universal phone-scam response

1. **Don't react to the alarm.** However scary or exciting the call, keep your feet on the ground. The emotion is the trap.
2. **Don't confirm or give any information** — not your name, not “yes,” not your birthday, nothing. “Who are you trying to reach?” is a fine reply.
3. **Hang up.** You never owe a caller an explanation. Just hang up.
4. **If you're worried it might be real, look up the real number yourself** — on your card, bill, or statement — and call to check. Never use a number the caller gave you.

TIP

When in doubt, just don't answer unknown numbers

You are never obligated to answer the phone. If you don't recognize a number, let it go to voicemail — a real person with real business will leave a message, and a scammer usually won't. Returning a call after listening to a calm voicemail, on a number you've verified, puts you completely in control. Silence is a perfectly good defense.

GOOD TO KNOW

Saying “yes” can be used against you

Some scam calls open with “Can you hear me?” or “Is this [your name]?” hoping to record you saying “yes.” It's wise not to answer questions from unknown callers with a plain “yes” — instead ask “who's calling?” or simply hang up. It's a small habit that closes off one more little trick.

CHAPTER 13

The Grandparent / Family Emergency Scam

This is one of the cruelest scams, because it turns your love for your family against you. It's also one to understand deeply right now, because new technology has made it far more convincing than it used to be.

How it goes

You get a frantic call: it's “your grandchild” (or a lawyer or officer calling on their behalf). They're in trouble — a car accident, an arrest, stuck abroad — and they need money *right now*, and they beg you **not to tell their parents** because they're ashamed. The voice is upset, rushed, and just plausible enough. They ask for gift cards, a wire, or cash by courier.

SCAM ALERT

The new danger: scammers can fake a loved one's voice

You should know this plainly: with today's technology, a scammer can take a few seconds of someone's voice from a video online and make a **convincing fake** that sounds like your grandchild or child on the phone. So “it really sounded like them” is no longer proof. This is unsettling, but the defense is simple and total — and it's in the next box.

The defense that never fails

1. **Hang up** — even if the voice sounds exactly right.
2. **Call your grandchild (or their parents) back directly** on the number you already have for them. You'll almost always find them safe and sound.
3. **Agree on a family “safe word”** in advance — a secret only real family knows — so you can ask “what's the safe word?” and catch any imposter instantly.

FROM BILL

This scam preys on the best thing about you

I hate this one, because it weaponizes your love. So let me give you permission in advance: if a call like this comes, it is *right and loving* to hang up and check, even if part of you fears the emergency is real. A real grandchild will forgive a five-minute delay while you verify. Set up a family safe word this week — it's one of the best protections there is. And if one of these calls ever rattles you, call me at (330) 200-8042.

CHAPTER 14

The “Tech Support” Call

Another extremely common one: a caller claims to be from **Microsoft, Apple, your internet provider, or a “security team,”** warning that your computer is infected, hacked, or sending out a virus. They sound official and concerned. It is always a scam.

How it unfolds

- They say they've “detected a problem” with your computer and need to “fix” it.
- They talk you into installing a program or visiting a website that gives them **remote control** of your computer.
- They show you harmless system messages and claim they're “viruses” to frighten you.
- They charge you for fake “repairs,” steal from accounts you log into, or demand gift cards.

SCAM ALERT

Real tech companies never call you about your computer

This one has a wonderfully simple tell: **Microsoft, Apple, Google, and your internet provider will NEVER call you out of the blue to say your computer has a virus.** They have no way to know, and they don't make such calls. Any call claiming this is 100% a scam, every time. Hang up. Don't press any button “to speak to support” — just hang up.

HEADS UP

Never let a caller connect to your computer

The heart of this scam is getting **remote access** — letting the stranger control your screen. Never, ever install software or type a code a caller gives you to “let them in.” Once they're in, they can rifle through your files, empty accounts, and lock you out. If you've already let someone in, turn off the computer, disconnect it from the internet, and call me right away — (330) 200-8042.

CHAPTER 15

Government Impersonation: IRS, Social Security, Police

Scammers love to pose as the government, because the words “IRS,” “Social Security,” and “police” carry fear and authority. Understanding how real agencies actually behave is your shield.

The common government scams

- **“You owe back taxes”** — a caller claiming to be the IRS threatens arrest or lawsuits unless you pay immediately, often by gift card.
- **“Your Social Security number has been suspended”** — a threat that your benefits or number are frozen due to “suspicious activity.”
- **“There's a warrant for your arrest”** — a fake officer says you missed jury duty or a court date and must pay a fine to avoid jail.
- **“Medicare is issuing new cards”** — a ploy to collect your Medicare or Social Security number.

STAY SAFE

How real agencies actually behave

Here's the truth that defeats all of these: **the IRS, Social Security, and the police do not call to threaten you, do not demand immediate payment, and are never paid in gift cards or wire transfers.** The real IRS contacts you first by *mail*. Your Social Security number cannot be “suspended.” Police do not phone you to collect fines over missed jury duty. Any call that does these things is a scam — hang up without a second thought.

If you're worried it might be real

If a fear nags that you might genuinely owe something, that's natural — and easily settled. Hang up, and contact the agency yourself using a number from your own records, a real bill, or the agency's official website (irs.gov, ssa.gov). You'll find there's no problem — or you'll handle a real one calmly, on your terms, with no threats and no gift cards. Either way, you've taken the scammer out of the picture.

CHAPTER 16

The Bank “Fraud Department” Call

A particularly convincing scam is a call from your “bank's fraud department” warning of suspicious charges. It feels helpful — they're protecting you! — which is exactly what makes it dangerous.

The trap

The “fraud department” says someone's trying to drain your account, and to “secure” your money they ask you to confirm your card number, your login, a texted code, or to **move your money to a “safe account”** they name. Every one of those requests is the actual theft in disguise — they're walking you through robbing yourself.

SCAM ALERT

Your bank never asks you to move money to a “safe account”

This is a bright, clear line: **no real bank will ever call and ask you to transfer your money to a different “safe” or “holding” account, nor ask you to read back a security code, nor ask for your full password.** Those are the scam, not the rescue. If your “bank” asks any of these, hang up and call the number on the back of your card to check — you'll find the “fraud” was the call itself.

The right way to check on your account

If a call makes you worry about your account, the fix is reassuringly simple: hang up and call the number printed on the **back of your bank card** or on your statement. That reaches the real bank, who can tell you in a moment whether anything's actually wrong (usually nothing is). You lose nothing by hanging up on a real bank and everything by staying on with a fake one.

FROM BILL

When a “bank” call spooks you, call me too

These bank-fraud calls are designed to panic you, and they're convincing — so if one ever gets your heart racing, you don't have to sort it out alone in the moment. Hang up, take a breath, and call me at (330) 200-8042 as well as your real bank. We'll calmly confirm your money is safe. There's no shame in a second opinion; it's the smartest move there is.

CHAPTER 16a

The Jury Duty / Warrant Scam

A frightening and common phone scam: a caller posing as a **sheriff's deputy or court officer** says you missed jury duty (or a court date) and there's now a **warrant for your arrest** — but you can avoid jail by paying a "fine" right now. It's designed to terrify law-abiding people into paying.

Why it's always false

- **Courts and police never call to collect fines** or threaten arrest over the phone.
- **Real missed-jury-duty matters come by mail,** and are handled in person, never by gift card or wire.
- **No real officer takes payment in gift cards** to "clear a warrant."

SCAM ALERT

You cannot pay away an arrest warrant by phone

The entire premise is false: the legal system does not work by a deputy phoning you for immediate payment to avoid jail. If you're ever truly unsure whether you missed jury duty, hang up and call the actual courthouse using a number from the official county website or phone book. You'll find there's no warrant — and you'll have calmly defused a scam built entirely on fear.

FROM BILL

This one scares people badly — call me and breathe

The fake-warrant call is especially cruel because it targets your respect for the law and your fear of jail. If one ever has your heart pounding, hang up and call me at (330) 200-8042 before doing anything. We'll confirm together, in two minutes, that it's a scam — and I'll be glad you called rather than carried that fear alone.

CHAPTER 16b

Utility and Service Shut-Off Scams

Another fear-based phone scam: a caller claims to be from your **electric, gas, or water company**, warns your service will be **shut off within the hour** for an unpaid bill, and demands immediate payment — you guessed it — by gift card or a strange app.

How real utilities actually operate

A genuine utility gives you **written notice well in advance** of any shut-off, accepts normal payment methods, and never demands gift cards or threatens to cut your power in the next hour if you don't pay a stranger over the phone. The rush and the gift cards are the scam, plain and simple.

STAY SAFE

Never pay an “urgent” utility bill to a caller

If a “utility” calls threatening immediate shut-off, don't pay and don't panic. Hang up and call the number on your actual **paper bill** or the company's official website to check your account. You'll almost always find you're paid up. Real utilities don't operate by surprise threats and gift cards — that combination is a scam every time.

TIP

Scammers strike in bad weather and heat waves

These shut-off scams spike during heat waves and cold snaps, when losing power feels especially frightening and people pay quickly out of fear. If you get such a call during extreme weather, be *extra* skeptical — the timing is deliberate. Your real utility won't leave you in the cold over a single phone call.

CHAPTER 16c

Voicemail, Callback, and “Survey” Traps

A few smaller phone tricks round out the picture. None is complicated, and the same habits defeat them all.

Traps to know

- **Alarming voicemails** — a recording about “your Social Security number” or “legal action” urging you to call back. Don't; it just connects you to the scammer.
- **Fake callback numbers** — numbers in texts or voicemails that reach the scam, not the real company.
- **“Quick survey” or “political poll” calls** that drift into asking for personal or financial details, or a “shipping fee” for a “free” reward.

GOOD TO KNOW

Always reach companies by a number YOU find

The thread running through all phone scams is that the scammer provides the number you call — so it reaches them, not the real company. Break that every time by looking up the number yourself: on your bill, your card, the official website, or the phone book. A number you found independently can't be a scammer's. Make this your unbreakable habit and the phone loses most of its danger.

WHAT THIS DOES FOR YOU

One habit retires a dozen phone scams

Notice how the same few habits — don't trust incoming calls, don't pay by gift card, hang up and verify on a number you found — defeat the grandparent scam, the tech scam, the IRS scam, the bank scam, the utility scam, and more. You're not memorizing a hundred defenses; you're mastering three or four that cover them all. That's a wonderfully manageable thing to carry.

CHAPTER 16d

Fake Debt Collectors

A caller claims you owe a debt — an old payday loan, a medical bill, a credit card — and threatens lawsuits, arrest, or wage garnishment unless you pay immediately. Sometimes it's a debt you've never heard of; sometimes it's a real old debt they've dug up to pressure you. Either way, the threats and the rush are the scam.

Your rights and the warning signs

- **Real debt collectors must send written notice** and follow strict rules; they can't threaten arrest.
- **Scammers refuse to put it in writing,** demand immediate payment by gift card or transfer, and won't give verifiable details.
- **You have the right to request written validation** of any debt before paying a cent.

SCAM ALERT

You can't be arrested for owing a debt — and real collectors don't threaten it

Two facts dissolve this scam: **you cannot be jailed for owing an ordinary debt,** and legitimate collectors must send written proof and follow the law — they don't demand gift cards or threaten arrest over the phone. If a “collector” threatens you or won't provide written validation, hang up. For any debt you're unsure about, request it in writing and check it against your own records before paying anything.

CHAPTER 16e

The “Your Car's Warranty” and Other Nuisance Calls

Some scam and junk calls are less about stealing your savings and more about wasting your time and fishing for a reaction — but a few hide real traps. The famous “warranty” robocall is the poster child.

Common nuisance calls

The call	What it really is
“Your car's warranty is expiring”	A robocall fishing for a payment or your details. Your car's maker doesn't robocall you.
“Lower your credit-card interest”	A “free” offer that charges a fee and harvests your card number.
“Final notice” about anything	Manufactured urgency — a hallmark of junk and scam calls.
Fake “charity” or “police fund” calls	Pressure to donate by card or gift card to a cause you can't verify.

TIP

You don't have to engage — hanging up is always allowed

For all of these, the answer is the same and wonderfully simple: **hang up.** Don't press buttons, don't argue, don't “ask to be removed” — just hang up, and block the number if you can. You owe a robocall nothing, not even politeness. The less you engage, the fewer calls you'll get, because engagement marks your number as “live.”

WHAT THIS DOES FOR YOU

A quieter phone, and a calmer mind

Between not answering unknown numbers, hanging up on junk, blocking repeat offenders, and turning on your phone's spam filters, you can dramatically quiet the flood of nuisance and scam calls — and with it, the little jolt of worry each one brings. You deserve a phone that serves you, not one that pesters you. These habits give you that peace.

PART 4

Email & Text Scams

Phishing by email and text — the fake delivery notice, the “account suspended” alert, the surprise invoice, the lottery win. How to read a message safely and never take the bait.

CHAPTER 17

Phishing: The Art of the Fake Message

Phishing (said “fishing,” and it means just that — fishing for your information) is a scam message, by email or text, pretending to be from someone you trust. It's the most common scam of all, and once you know the pattern, you'll spot them easily.

What phishing messages are after

- **Your passwords** — by sending you to a fake login page that looks real.
- **Your money or card details** — via a fake payment or “verify your card” page.
- **Your personal information** — Social Security number, date of birth, account numbers.
- **Control of your device** — by getting you to click a bad link or open a harmful attachment.

GOOD TO KNOW

They only win if you click or reply

Here's a comforting truth: a phishing message sitting in your inbox can't hurt you by itself. The danger is only in **clicking its link, opening its attachment, or replying with information.** So the whole defense comes down to one habit: don't click, don't open, don't reply — unless you were genuinely expecting the message and trust who it's from. Simply reading and deleting a suspicious message is perfectly safe.

CHAPTER 18

The Red Flags in a Message

Scam emails and texts give themselves away if you know what to look for. Here are the tells that should make you stop before you touch a single link.

The message red flags

- **Urgency or threat** — “act now,” “your account will be closed,” “final notice.”
- **A link or button to “verify,” “confirm,” or “unlock”** something.
- **A generic greeting** — “Dear Customer” instead of your name.
- **Odd spelling or grammar,** or a slightly-wrong company name.
- **A sender address that doesn't match** — the name says “Amazon” but the real address is gibberish (tap the sender to reveal it).
- **An unexpected attachment,** especially one you weren't waiting for.
- **A request for information** no real company would ask by email — password, full card number, Social Security number.

HEADS UP

Hover or press-and-hold to see where a link really goes

A link's visible words can say one thing while it leads somewhere else entirely. On a computer, rest your mouse pointer over a link (without clicking) to see the true destination at the bottom of the screen; on a phone, press and hold the link to preview it. If the real address isn't the genuine company's website, don't go there. Better still — don't use the message's link at all; visit the company yourself.

The golden rule for links

Here's the habit that defeats nearly every phishing message: **never use a link in an unexpected message to reach an account or company.** If an email says there's a problem with your bank, your Amazon order, or your Netflix, don't click — instead, open the app or type the website yourself and check there. If the problem is real, you'll see it; if it was a scam, you'll have sidestepped it entirely.

CHAPTER 19

The Fake Delivery Notice

One of the most common text and email scams right now is the **fake package notice** — because almost everyone is expecting *some* delivery, so it feels plausible.

How it looks

A text or email claiming to be from **USPS, UPS, FedEx, DHL, or Amazon** says your package is **held, delayed, or needs a small fee or address confirmation** — with a link to "reschedule" or "pay." The link leads to a fake page that steals your card details or personal information.

SCAM ALERT

Carriers don't text you for a fee or your card details

Real delivery companies don't send surprise texts demanding a small payment or your card number to release a package. If you're genuinely expecting something, check it the right way: go to the carrier's real website yourself, or your Amazon **Your Orders** page, and track it there. Never click the link or pay the "fee" in the message. When in doubt, it's a scam.

Why these catch people

This scam works on timing and coincidence — send enough "missed delivery" texts and plenty will land on someone who really is awaiting a parcel. Don't let the coincidence fool you. The fact that you *are* expecting a package doesn't make a surprise fee-demanding text real. Track your actual order through the real app, and ignore the text.

CHAPTER 20

“Your Account Has a Problem”

Another everyday phishing theme: a message warning that one of your accounts — bank, Amazon, Apple, Netflix, PayPal, your email — is **locked, suspended, or showing suspicious activity,** and you must click to “verify” or “reactivate.”

The trick

The link leads to a counterfeit login page — often a very good copy — designed to capture your username and password the moment you type them. With those, the scammer walks into your real account. The whole scheme hinges on you trusting the message enough to sign in through *its* link.

STAY SAFE

Reach your accounts your own way, never through a message

The defense is a single unbreakable habit: **to check any account, go there yourself** — open the app you already have, or type the website address yourself — never through a link in a message warning of a problem. If your account truly has an issue, you'll see it when you log in normally. If the warning was a scam, you've quietly avoided handing over your password. This one habit stops nearly all account-phishing cold.

A special word on your email account

Guard your **email** password most fiercely of all. Because password resets for your other accounts get sent *to your email*, a scammer who captures your email login can reach much of your life. Protect it with a strong, unique password and two-step verification, and be extra skeptical of any “your email account is at risk” message. See the Email manual in this series for more.

CHAPTER 21

Lottery, Prize, and “Free Money” Scams

Not all scams frighten you — some delight you. The **prize scam** says you've won a lottery, a sweepstakes, a gift card, or an inheritance, and all you must do is pay a small “fee” or “tax” or confirm your details to collect. It's a trick as old as the hills, dressed in new clothes.

Why it's always false

- **You can't win a lottery you never entered.** If you didn't buy a ticket, there's no prize.
- **Real prizes never require you to pay to receive them.** Any “fee” or “tax” you must pay first is the scam.
- **Real winnings don't come by surprise text or email** demanding secrecy and speed.

SCAM ALERT

If you have to pay to collect it, it's a scam

Here's the one-line rule that kills every prize scam: **you never have to pay money to receive money you've genuinely won.** The moment a “prize” requires a fee, a tax, gift cards, or your bank details up front, it is a scam — without exception. Real windfalls don't work that way. Delete it, and don't let the excitement override your common sense.

TIP

Excitement is a red flag too, not just fear

We spend a lot of time guarding against scary scams, but the *happy* ones are just as dangerous, because joy lowers your guard the same way fear raises your panic. A sudden thrill — “I've won!” — should trigger the very same pause as a threat. When something feels too good to be true, let that good feeling be your warning, and check before you act.

CHAPTER 21a

Dangerous Attachments

Beyond links, scam emails sometimes carry **attachments** — files clipped to the message — that can harm your computer if you open them. A little caution here keeps you safe without making you fear every file.

Attachments to be wary of

- **Unexpected files** of any kind, especially from senders you don't know.
- **Files ending in .zip, .exe, .scr** you weren't expecting — these can run harmful programs.
- **A “document” that asks you to “enable content” or “enable macros”** when you open it — don't.
- **A surprise “invoice,” “receipt,” or “resume”** from a stranger — a classic way to deliver a harmful file.

HEADS UP

Don't open an attachment you weren't expecting

The simple rule: only open an attachment when you were genuinely expecting it from someone you trust. An unexpected file — even one that appears to come from a friend — deserves a pause; if it seems odd, call them to ask if they really sent it (their email may have been hijacked). When in doubt, don't open it, and delete the message. A file you never open can't hurt you.

CHAPTER 21b

Unsubscribe Traps and Reply Bait

A subtle point that trips people up: with *junk you don't recognize*, even the innocent-looking actions — clicking “unsubscribe,” or replying “stop” — can work against you.

Why these can backfire

For a **legitimate newsletter you once signed up for**, Unsubscribe is safe and useful. But on **junk from an unknown sender**, clicking Unsubscribe or replying at all simply tells the scammer your address is live and read by a real person — inviting a flood more, and sometimes leading to a bad link. The scammer put that “unsubscribe” there hoping you'll engage.

TIP

Recognize the sender? Unsubscribe. Don't? Just report as spam

Here's the clean rule: use **Unsubscribe only on mail from senders you recognize and once trusted.** For junk from total strangers, don't click anything — just mark it as spam and delete it. Reporting it as spam trains your email to filter similar messages without tipping off the sender that you're there. See the Email manual for more on taming junk.

GOOD TO KNOW

Silence is the best answer to a stranger's junk

With unknown junk and scams, the most powerful response is often to do nothing at all — no click, no reply, no unsubscribe. Report it as spam and delete it. Every interaction, however small, is information the scammer can use; silence gives them nothing. When it comes to strangers' junk, not engaging is engaging wisely.

CHAPTER 21c

Business and Invoice Email Scams

A costly category, especially if you run a small business, a club, or a church: scams that target **payments and invoices** by email. Even for personal use, it's worth knowing, because versions of it reach everyone.

The common forms

- **Fake invoices** — a bill for a subscription, antivirus renewal, or service you never bought, hoping you'll pay or call the “billing” number to dispute it (which reaches the scammer).
- **“Your subscription auto-renewed for $499”** — alarm designed to make you call and hand over card details to “cancel.”
- **Changed payment details** — a message pretending to be a vendor or contractor asking you to send a payment to a “new” bank account.

SCAM ALERT

Verify any surprise bill through your own records

If a bill or renewal notice surprises you, **don't call the number or click the link in the message.** Check your own records: your bank statement, your actual account on the real company's website, your order history. A genuine charge will be there; a fake one won't. And **never** pay a new or changed invoice to a different account on an email's say-so without confirming by a phone number you already trust.

FROM BILL

Unsure about a bill or charge? Let's look together

Surprise “invoices” and “auto-renewal” emails are designed to make you panic and call their number. Don't. Bring it to me instead — (330) 200-8042 — and we'll check your real accounts and statements together to see whether it's genuine (it usually isn't). Two minutes of checking beats a rushed call to a scammer's “billing department” every time.

CHAPTER 21d

How to Check Who Really Sent an Email

A single skill catches a huge share of email scams: looking past the friendly *name* on a message to the real *address* behind it. Scammers can put any name they like on an email, but the true address is much harder to fake and often gives them away.

Revealing the real sender

1. Open the message and look at the top, where it shows who it's from.
2. **Tap or click the sender's name** (on a phone, tap the name or the little arrow beside it).
3. The **true email address** appears — for example, the name says “Amazon” but the real address is no-reply@random-xyz.com.
4. Ask: does this address genuinely belong to the company it claims to be? If it's gibberish or the wrong website, it's a fake.

TIP

The name is a costume; the address is the face

Think of the sender's name as a costume anyone can put on, and the actual email address as the face underneath. A scammer can dress up as “Your Bank,” but when you lift the mask and the address is xk92@mail-ru.net, the disguise falls away. Make a habit of glancing at the real address on any message that asks you to click or act — it's a two-second check that unmasks many scams.

HEADS UP

Even a right-looking address isn't total proof

Clever scammers sometimes forge an address that looks correct, or use a tiny misspelling (amaz0n.com with a zero, or paypaI with a capital i). So checking the address is a powerful filter, but not a guarantee. That's why the deeper rule still rules: don't act through a message's links at all — reach the company yourself, the way you always do. The address check catches the obvious fakes; your own habits catch the rest.

CHAPTER 21e

Spam vs. Scam: Knowing the Difference

Not every piece of junk mail is a scam, and telling them apart helps you respond correctly and worry less. Both are unwanted, but one is merely annoying while the other is dangerous.

The difference

Type	What it is
Spam (junk)	Unwanted advertising — real companies, pushy marketing. Annoying, but not trying to rob you.
Scam	A deliberate trick to steal money, information, or access. Dangerous, dressed up as something trustworthy.

Much of what lands in your spam folder is merely marketing you didn't ask for — harmless if ignored. The scams are the ones that impersonate someone you trust and try to get you to *act*: click, call, pay, or reveal. Both can simply be deleted; the scam just deserves an extra beat of recognition so you never take its bait.

GOOD TO KNOW

For both, the safe response is the same: don't engage, delete

Here's what makes this easy: whether a message is mere spam or an outright scam, the safe response is identical — **don't click its links, don't reply, mark it as spam, and delete it.** You don't have to perfectly diagnose which is which. Treat all unwanted, unexpected messages the same cautious way, and you're protected from both the annoyance and the danger.

WHAT THIS DOES FOR YOU

A tidy, safe inbox is within your reach

Between your email's automatic spam filter, the habit of reporting junk, and your eye for the red flags, you can keep your inbox both tidier and far safer. The junk gets filtered, the scams get spotted, and the real mail from the people you love comes through clean. That's a calmer, safer daily experience — and it's entirely achievable.

PART 5

Computer & Pop-Up Scams

The alarming pop-up that freezes your screen and tells you to call a number — and the “tech support” takeover it leads to. How to recognize these, and exactly what to do when one appears.

CHAPTER 22

The Scary Pop-Up

You're browsing along when suddenly your screen is taken over by a **frightening warning**: “YOUR COMPUTER IS INFECTED,” often with flashing colors, a loud alarm sound, and a phone number to call “immediately” for help. Your heart jumps. That reaction is exactly what the scammer wants — and the whole thing is fake.

What's really happening

This is just a **web page designed to look like a system warning.** It hasn't detected anything; it can't. It's a piece of theater — scary pictures and sounds — built to panic you into calling the number, where a fake “technician” waits to take over your computer and your money. Your computer is fine. Nothing is infected. It's a billboard, not a diagnosis.

SCAM ALERT

A pop-up with a phone number to call is ALWAYS a scam

Memorize this: **a real virus warning never, ever gives you a phone number to call.** Your actual security software quietly handles threats in the background. So any pop-up, alarm, or full-screen warning telling you to “call this number for support” is 100% a scam, every single time. Don't call it. Don't let the noise and colors rush you — it's all for show.

Why they use fear and noise

The flashing, the siren, the “do not restart your computer” warnings — all of it exists to stop you thinking and make you grab the phone. The instant you recognize it for the performance it is, the fear drains away and it becomes almost laughable. Knowing it's fake is the entire cure.

CHAPTER 23

What to Do When a Pop-Up Strikes

Let's make this practical, because a scary pop-up *will* likely happen to you one day, and knowing the steps in advance means you'll handle it calmly instead of in a panic.

Your calm, step-by-step response

1. **Don't call the number.** Don't click anything *inside* the pop-up — not “close,” not “OK,” not “scan now” (those can be traps too).
2. **Close the web page or browser.** Try the X on the browser tab, or close the whole browser program.
3. **If it won't close, restart the computer.** Hold the power button to turn it off, wait, and turn it back on. (Yes, despite what the pop-up says — restarting is safe and clears it.)
4. **When it reopens,** if your browser offers to “restore” the pages, decline, so the bad page doesn't come back.

TIP

Restarting almost always clears a stuck pop-up

If a pop-up has “frozen” your screen and won't go away, the humble restart is your friend — turn the computer fully off and on again. It ignores the pop-up's “don't restart!” warnings (those are the scam talking) and brings you back to a clean screen. Nothing is lost, and the fake warning is gone. It's the gentlest, surest fix.

HEADS UP

Even the “X” or “Close” can be a trick

On some fake pop-ups, every part of the page — including what looks like the close “X” or a “Cancel” button — is actually a clickable trap. That's why the safest move is to close the whole browser or restart, rather than hunting for a close button within the pop-up. When a warning fills your screen, don't play its game at all; back out entirely.

CHAPTER 24

If You Let Someone Into Your Computer

Sometimes, despite everything, a convincing “technician” talks someone into granting remote access before they realize it's a scam. If that's happened to you or a loved one, don't panic and don't feel ashamed — act. Quick steps limit the harm.

What to do right away

1. **Disconnect from the internet** — unplug the network cable or turn off Wi-Fi — to cut the scammer's access immediately.
2. **Turn the computer off.**
3. **From a different device,** change the passwords to your important accounts — especially email and banking.
4. **Call your bank** if you entered any financial details or made any payment, to watch for or stop fraud.
5. **Get the computer checked** by someone you trust before using it again, in case they left harmful software behind.

> **FROM BILL**
>
> **Let someone in by mistake? Call me — we'll make it right**
>
> If you've let a scammer onto your computer, the most important thing is to act fast and without shame — this happens to careful people constantly. Disconnect it, and call me at (330) 200-8042. I'll help you secure your accounts, check the computer for anything they left behind, and make sure you're safe again. The sooner we act, the less they can do. You are not in trouble, and you're not alone.

Watch for the “refund” follow-up

A cruel twist: weeks or months later, victims of a tech-support scam often get a call offering a **“refund”** for the earlier scam — which is the *same* crooks coming back for a second bite. They “accidentally refund too much” and ask you to send the difference back in gift cards. It's a scam on top of a scam. If you've been hit once, be especially wary of anyone offering to recover your money (see Part 7).

CHAPTER 25

Fake Antivirus and “Tune-Up” Software

Related to pop-ups is a quieter scam: **fake security or “speed-up” software**. A pop-up or ad urges you to download a program to “clean,” “protect,” or “speed up” your computer — and the program itself is the problem.

How it works

You install the “helpful” program; it runs a dramatic “scan” and reports dozens of scary (invented) problems, then demands payment to “fix” them. Some of these programs also slow your computer, bombard you with ads, or quietly spy on you. You've paid for a problem instead of a solution.

HEADS UP

Don't install software a pop-up or ad pushes on you

Only install programs you deliberately sought out from a source you trust — your device's official app store, or a well-known company's real website you typed yourself. Never install something because a pop-up, ad, or alarming message told you to. If your computer genuinely needs cleaning up or protecting, that's a job for trusted, built-in tools or a real person, not a flashing advertisement.

GOOD TO KNOW

Your computer already has good protection built in

Here's a relief: modern Windows and Mac computers come with solid, free security built right in (Windows Security, and the Mac's own protections), kept up to date automatically. For most folks, that's plenty — you don't need to buy or download extra “antivirus” programs, and you certainly shouldn't install one a pop-up is pushing. If you're unsure whether you're protected, ask me; the answer is usually “you already are.”

CHAPTER 25a

The Fake “Support Number” You Find by Searching

Here's a sneaky one that catches careful people: you have a real problem — a printer won't work, you're locked out of an account — so you **search the web for the company's help number**. But some of the numbers that appear are **scammers who've planted fake “customer support” listings and ads**. You call thinking you've reached the real company, and walk straight into a trap.

Staying safe when you need help

- **Get support numbers from the company's own official website** (type the address yourself) or from your paperwork — not from a search result or ad.
- **Be wary of numbers in sponsored ads** at the top of search results.
- **A “support” agent who wants remote access or gift-card payment** is a scammer, no matter how you found them.

HEADS UP

The support number itself can be the scam

This flips the usual advice, so note it carefully: even when *you* go looking for help, the number you find might be a scammer's plant. Always get support contacts from the real company's official website or your original paperwork — never from a search ad or a random listing. And the giveaway remains the same: a genuine support line never needs remote control of your computer or payment in gift cards.

FROM BILL

Need a real support number? I'll help you find it

Hunting down a legitimate customer-support line is exactly where people stumble into fake-support scams. If you need to reach a company's real help desk and aren't sure you've got the right number, call me first — (330) 200-8042 — and I'll help you find the genuine one. It's a small thing that heads off a nasty trap.

CHAPTER 25b

Fake Updates and “Your Device Is Infected” Apps

While browsing, you may see a message urging you to **“update your browser,” “update Flash,”** or install an app to “fix” or “protect” your device. These fake update prompts are a common way to trick people into installing harmful software.

Real updates vs. fake ones

- **Real updates** come from your device itself (its Settings) or its official app store — not from a web page or pop-up while you browse.
- **Fake update prompts** appear as flashy web-page messages, often mimicking a system window.
- **When in doubt, close the page** and check for updates the proper way: in your device's Settings, or the App Store / Play Store.

STAY SAFE

Update only from Settings or the official store — never a pop-up

Make this a firm habit: install software and updates only from your device's own **Settings** or its official **app store**, which you open yourself. Never install anything because a web page or pop-up told you to — that's how harmful software gets in. If you're ever unsure whether your device needs a real update, ask me; keeping devices updated the proper way is one of your best protections, and it's easy to do safely.

GOOD TO KNOW

Keeping devices updated — the right way — is good protection

Don't let fake update scams sour you on *real* updates, which genuinely matter: they patch the security holes scammers exploit. The key is *where* the update comes from. A prompt inside your phone's Settings or the App Store is real and good; a flashy “update now!” on a web page is a trap. Same word, opposite meaning — and the source tells you which is which.

CHAPTER 25c

Public Wi-Fi and Charging Cautions

A couple of quieter risks when you're out and about. Neither is cause for alarm, but a little awareness keeps you safe on the road.

Out-and-about habits

- **On public Wi-Fi** (coffee shops, airports), avoid logging into your bank or entering card details — others on the same network could potentially snoop. Use your phone's own cellular connection for sensitive things.
- **Be cautious with public USB charging stations** — use your own charger in a wall outlet, or a plain power bank, rather than an unknown USB port.
- **Don't leave devices unlocked** or unattended in public.

TIP

For anything sensitive, use your own cellular data

A simple safe habit when you're out: for banking, shopping, or anything involving passwords or money, use your phone's **own cellular data** rather than public Wi-Fi. Your cellular connection is private to you, while public Wi-Fi is shared. For casual browsing, public Wi-Fi is fine — just save the sensitive business for your own connection or home.

WHAT THIS DOES FOR YOU

A little awareness, total freedom to roam

None of this should keep you home or make you nervous with your devices in public — just the opposite. A couple of easy habits (sensitive tasks on your own data, your own charger) let you use your phone freely and safely anywhere you go. Awareness isn't fear; it's what lets you enjoy your technology out in the world without a second thought.

CHAPTER 25d

Fake Websites and Login Pages

Many scams funnel you to a **fake website** — a counterfeit copy of a bank, a store, or a login page — built to capture whatever you type. These copies can be very good, so a few checking habits are worth having.

Spotting a fake site

- **Check the web address** at the top carefully — look for misspellings (amaz0n.com), extra words (amazon-security.com), or the wrong ending (.net instead of .com).
- **You arrived via a link in a message** — the single biggest warning. Reach sites yourself instead.
- **It asks for too much** — a login page suddenly wanting your full card number, Social Security number, or PIN.
- **Something looks slightly off** — fuzzy logos, odd wording, broken links.

HEADS UP

A padlock doesn't mean a site is honest

You may have heard to “look for the padlock” in the address bar. It's worth knowing that the padlock only means the connection is encrypted — **it does not mean the site is genuine or safe.** Scammers' fake sites can have padlocks too. So don't rely on it. The real protections are checking the exact web address and, above all, reaching sites yourself rather than through a message's link.

TIP

Type it yourself, or use a saved bookmark

The surest way never to land on a fake login page is to reach your important sites the same way every time: type the address yourself, or use a **bookmark** you saved from the real site. Then you always arrive at the genuine page, no matter what links the scammers send. Setting up bookmarks for your bank and key accounts is a lovely little safety project we can do together.

CHAPTER 25e

Keeping Your Web Browsing Safe

A few gentle habits while browsing the web keep you clear of most online traps, without making you afraid to explore and enjoy the internet.

Safe browsing habits

- **Be wary of ads,** especially flashy ones promising prizes, miracle cures, or shocking news. Don't click.
- **Stick to known, reputable websites** for shopping and important business.
- **Don't download files or programs** except from official sources you sought out.
- **Close pop-ups by closing the page or browser,** not by clicking inside them.
- **Keep your browser and device updated** (the proper way, via Settings).

GOOD TO KNOW

Most of the web is safe — a little care handles the rest

Let's keep this in perspective: the vast majority of the internet is perfectly safe to browse and a genuine joy to explore — news, recipes, old friends, your interests, the whole world at your fingertips. A handful of easy habits handles the small risky corner. So browse freely and curiously; you don't need to be nervous, just sensible. Caution is the seatbelt that lets you enjoy the drive.

FROM BILL

Want a safer, simpler browsing setup? Let's do it

If you'd like, we can set up your web browser to be both safer and easier — bookmarks for your important sites, a pop-up blocker turned on, your home page set to something pleasant, and the clutter cleared away. It makes the whole internet feel friendlier and less risky. Call (330) 200-8042 and we'll tidy it up together.

PART 6

Online Scams

The schemes that unfold over days and weeks: the online romance, the “can't-miss” investment, the too-cheap online store, the fake charity. These take patience to run — and a little awareness to avoid.

CHAPTER 26

Romance Scams

This is among the most painful scams, because it steals not just money but trust and affection. A **romance scam** is a fake relationship, built patiently online over weeks or months, with the sole aim of eventually asking you for money. I'll speak about it gently, because the people it targets are warm-hearted and deserving of love — which is exactly why scammers choose them.

How these scams unfold

- They meet you on a dating site, social media, or even a stray "wrong number" text that turns friendly.
- They're attentive, affectionate, and move quickly to declarations of love — but always have a reason they **can't meet in person or video chat**.
- After trust is built, a **crisis** appears: a medical bill, a stuck shipment, a business emergency, travel money to finally visit you.
- They ask for help — and once you send money, the "emergencies" never stop.

HEADS UP

Won't meet in person or on video? That's the tell

The clearest sign of a romance scam is simple: after weeks or months of devotion, the person still **will not meet you face to face or on a live video call** — there's always an excuse (overseas work, the military, a shy nature). A genuine partner finds a way to be seen. If someone professes love but perpetually can't show their live face, and then asks for money, it is a scam, however much your heart wishes otherwise.

STAY SAFE

Never send money to someone you haven't met in person

Here is the firm, loving rule: **never send money, gift cards, or your financial details to a romantic interest you have not met in person** — no matter how real the feelings seem or how urgent the crisis. Real love does not arrive as a request for a wire transfer. If you're unsure about an online relationship, please talk to a trusted friend, a family member, or me. There's no judgment — only care for your heart and your savings.

A word of compassion

If you're in a relationship like this, or have been, please hear this: wanting companionship is a beautiful, human thing, and being deceived by someone who exploited it is *their* crime, not your failing. Many wonderful, intelligent people have been caught. Reaching out to someone you trust isn't an admission of foolishness — it's an act of strength.

CHAPTER 27

Investment and Cryptocurrency Scams

Investment scams promise big, safe, fast returns — often involving cryptocurrency, gold, or "exclusive" opportunities — and they're responsible for some of the largest losses of all, because people invest their life savings. They've grown more sophisticated, so they're worth understanding.

The warning signs

- **Guaranteed or unusually high returns** with "little or no risk" — real investing never guarantees this.
- **Pressure to act fast** before a "limited opportunity" closes.
- **A "mentor," "advisor," or new online friend** who introduces the opportunity — often the same person as a romance scam.
- **A slick website or app showing your "profits" growing** — fake numbers designed to tempt you to invest more.
- **You can "withdraw" a small amount at first** (to build trust), but larger withdrawals are blocked or taxed.

SCAM ALERT

"Guaranteed high returns" is a contradiction — and a scam

A bedrock truth of money: **higher returns always mean higher risk, and no legitimate investment guarantees big profits.** Anyone promising safe, fast, guaranteed returns — especially in crypto, and especially someone who contacted you — is lying. The fake app showing your money "growing" is just a picture. Never invest based on an online stranger's urging, and never through a "crypto ATM" a caller directs you to.

FROM BILL

Thinking of a new investment? Run it past someone first

Before putting money into any opportunity that reached you online or by phone — especially crypto — please talk it over with someone impartial: a family member, a licensed financial advisor you found independently, or me. I'm not a financial advisor and won't tell you what to invest in, but I can help you spot whether the *opportunity itself* bears the marks of a scam. A single conversation has saved people their entire retirement. Call (330) 200-8042.

CHAPTER 28

Online Shopping and Marketplace Scams

When buying and selling online — on marketplaces, social media, or unfamiliar websites — a little caution keeps you from fake stores and cheating buyers and sellers.

Common shopping scams

- **Fake online stores** — a slick website or social-media ad selling popular goods cheaply; you pay and nothing arrives.
- **Too-good-to-be-true prices** on brand-name items — a lure for counterfeits or pure theft.
- **Marketplace overpayment** — a "buyer" sends a too-large payment and asks for the difference back (a fake-check trick).
- **"Pay me off the platform"** — a seller or buyer asking to move off the official site to an untraceable payment.

STAY SAFE

Pay safely, and keep deals on the official platform

Protect yourself when shopping online: favor well-known retailers, pay with a **credit card** (which lets you dispute fraud), and **never** pay a stranger by gift card, wire, or a payment app for a purchase. On marketplaces, keep all payment and messaging *on the official platform* — the moment someone wants to take the deal "off-platform" or pay an unusual way, walk away. See the Amazon manual for safe-shopping details.

Spotting a fake store

Before buying from an unfamiliar website, pause and look: Is there a real company name, address, and phone number? Do the prices seem impossibly low? Is there a flood of suspiciously perfect reviews, or none at all? Did the site arrive via a social-media ad promising deep discounts? When several of these line up, close the page. A missed bargain costs nothing; a fake store costs you your money and your card details.

CHAPTER 29

Charity, Medicare, and Other Impersonations

A few more impersonation scams round out the picture — schemes that borrow the good name of charities, Medicare, or utilities to catch you off guard.

Scams that wear a trusted uniform

The scam	The reality
Fake charities	Especially after disasters — urgent pleas to donate, often by gift card or wire. Give only to charities you seek out yourself.
Medicare / health scams	Calls offering "free" braces, tests, or new cards to harvest your Medicare number. Medicare doesn't cold-call like this.
Utility shut-off threats	"Pay now or we cut your power today" — by gift card, naturally. Real utilities give written notice and don't take gift cards.
Jury duty / warrant	A "deputy" says you missed jury duty and must pay a fine to avoid arrest. Courts never collect fines by phone.

STAY SAFE

Give and pay on your own initiative, never on someone else's

A pattern unites all of these: someone *contacts you* and pressures you to give money or information right now. The safe habit is to flip it around — **donate, pay bills, and handle health matters on your *own* initiative,** through organizations and numbers you looked up yourself. When a "charity," "Medicare," or "utility" reaches out first and rushes you, treat it as a scam until you've verified it independently.

TIP

Protect your Medicare number like a credit card

Your **Medicare number** is valuable to scammers, who use it to bill for fake services. Guard it as you would a credit card: don't give it to anyone who calls you offering "free" equipment or services, and check your Medicare statements for charges you don't recognize. If you spot something odd, report it — the back of this book points you to where.

CHAPTER 29a

Social Media Scams

Facebook, Instagram, and the like are wonderful for staying close to family — and, unfortunately, fertile ground for scammers who use them to reach you with a friendly face. Knowing the common tricks lets you enjoy social media safely.

Scams that live on social media

- **Cloned accounts** — a scammer copies a friend's photo and name, "friends" you, then asks for money or pushes a "grant" or investment.
- **Too-good giveaways and quizzes** — "win a free RV!" or quizzes that harvest personal details (which double as password security answers).
- **Marketplace scams** — fake listings, deposits for rentals or pets that don't exist.
- **"Government grant" and "get-rich" messages** from "friends" whose accounts were hijacked.

HEADS UP

A "friend" asking for money may be a hijacked account

If a friend or relative messages you on social media asking for money, gift cards, or to click a link — even from their real-looking account — **check by contacting them another way** (a phone call) before doing anything. Accounts get hijacked constantly, and "I'm in trouble, send money" from a friend's profile is a classic scam. The real friend will be glad you checked.

TIP

Lock down your social media privacy

Scammers mine social media for details to make their tricks convincing and to guess your passwords. Setting your profile to **private** (friends only), and being thoughtful about sharing your birthday, hometown, and pets' names publicly, quietly starves them of material. It's a worthwhile little tidy-up — ask me and we'll review your privacy settings together.

CHAPTER 29b

Fake Jobs and Work-from-Home Scams

Offers of easy money from home — “mystery shopper,” “package reshipping,” “envelope stuffing,” “personal assistant” — are a long-running scam that's found new life online. They prey on the wish for a little extra income.

The warning signs

- **You're “hired” with no real interview,** often by text or chat.
- **They send you a check** to “buy supplies” or “test a service,” and ask you to send part back — the fake-check trick.
- **The “job” involves receiving and reshipping packages or forwarding money** — that's moving stolen goods or money (see the “mule” warning in Part 2).
- **They ask you to pay upfront** for “training,” “equipment,” or a “kit.”

SCAM ALERT

A real job never sends you a check to deposit and forward

Two bright-line rules for job offers: **a legitimate employer never sends you a check to deposit and then asks you to send money back, and never asks you to pay upfront for the privilege of working.** Both are classic scams — the check is fake and will bounce after you've sent real money. If a “job” involves either, walk away. Honest work pays *you*, not the other way around.

GOOD TO KNOW

Reshipping and money-forwarding “jobs” can make you a criminal

Be especially wary of “jobs” that have you receive packages and reship them, or receive money and forward it. These use you to launder stolen goods or funds — you could face real legal trouble, and you'll never be paid. No legitimate employer operates this way. If an offer involves forwarding packages or money, decline firmly and report it.

CHAPTER 29c

Too-Good Deals: Pets, Rentals, and Timeshares

A cluster of scams share one lure: an offer that's wonderfully cheap or convenient, requiring only a deposit or fee sent before you can see what you're buying. The deposit vanishes, and so does the “seller.”

Common too-good-to-be-true deals

The deal	The catch
Puppy / pet scams	An adorable pet at a low price, sold online sight-unseen, with a deposit by gift card or app. The pet doesn't exist.
Rental scams	A lovely apartment or vacation rental, cheap, with a deposit demanded before you can view it. It's not theirs to rent.
Timeshare “resale”	An offer to sell your timeshare or give you a “guaranteed buyer” — for an upfront fee that's the scam.
Car / big-ticket deals	A great price, but the seller insists on a wire or gift cards and won't let you inspect in person.

STAY SAFE

Never send a deposit for something you haven't seen in person

The thread through all of these: you're asked to **pay before you can see or verify** what you're getting, often by gift card, wire, or app. Don't. For pets, rentals, cars, and the like, insist on seeing the real thing in person (or via a live video call you arrange), pay by a method with protection, and walk away from anyone who rushes you or demands untraceable payment up front. A real seller won't mind your caution.

FROM BILL

Tempted by a deal that seems too good? Run it by me

If you've found a deal that seems wonderful but something's nagging — a deposit required, a seller who won't meet, a price that's startlingly low — that nagging is worth a phone call before you pay. Call me at (330) 200-8042 and we'll look at it together. A missed deal costs nothing; a scam deposit is gone for good.

CHAPTER 29d

Sweepstakes, Lotteries, and “You're Pre-Approved”

We touched on prize scams earlier; here are a few more “good news” scams that use excitement rather than fear, because they're common enough to deserve naming.

The happy-sounding traps

- **Foreign lottery / sweepstakes** — you've “won” something you never entered, abroad; just pay the “taxes” or “fees” first.
- **“Publishers” prize patrols** impersonating well-known sweepstakes, asking for a fee to “release” winnings.
- **“Pre-approved” loans or grants** requiring an upfront “processing” or “insurance” payment.
- **Inheritance from a “distant relative”** or stranger, needing fees to unlock.

SCAM ALERT

Legitimate winnings and grants never require an upfront fee

Across all of these, the tell is identical and ironclad: **you never pay to receive money you've won, been granted, or inherited.** Taxes on real winnings are handled with the IRS afterward, never prepaid to the “prize” company in gift cards. Any “good news” that requires you to send money first is a scam. Let the excitement be your warning, and delete it.

WHAT THIS DOES FOR YOU

Keep your optimism — just verify before you celebrate

None of this means becoming a cynic who trusts nothing good. It means pairing your hope with a simple check: real good fortune survives a pause and a second opinion; a scam falls apart under both. So enjoy life's genuine windfalls — just confirm they're real before you celebrate or, heaven forbid, pay a “fee.” Optimism and caution make fine companions.

CHAPTER 29e

Giving to Charity Safely

Generosity is a wonderful thing, and most charities are genuine and worthy. But scammers exploit kind hearts — especially after disasters — with fake charities and high-pressure pleas. A little care lets you give freely while making sure your money reaches real good.

Safe giving habits

- **Give on your own initiative,** to charities you know and seek out yourself — not in response to a surprise call, text, or door-knock that rushes you.
- **Be wary of copycat names** that sound like famous charities but aren't.
- **Never donate by gift card or wire** — real charities take checks and cards; scammers want the untraceable methods.
- **Check a charity** at a site like charitynavigator.org before giving to an unfamiliar one.

STAY SAFE

Real charities don't pressure you or take gift cards

A genuine charity is grateful for a gift whenever you choose to give it, in normal ways, with no pressure. A “charity” that calls out of the blue, rushes you, resists questions, or wants gift cards is a scam wearing a halo. Give on your own terms, to causes you've chosen and verified, and your generosity does exactly the good you intend — no scammer in the middle.

WHAT THIS DOES FOR YOU

Keep your generous heart — just point it carefully

The goal here isn't to make you stingy or suspicious of every good cause — the world needs your generosity. It's simply to make sure your gifts land where you mean them to. Give warmly and often, on your own initiative, to charities you trust, and your kindness does real good while the scammers get nothing. That's generosity with its eyes open.

PART 7

Protecting Yourself & Recovering

Building your everyday defenses, locking down your accounts and credit, what to do the moment you suspect a scam, how to report it — and the gentle art of helping a loved one stay safe.

CHAPTER 30

Your Everyday Defenses

Spotting scams is the main skill, but a few standing habits and settings make you a hard target in the first place. Think of these as locking your doors — simple, once-done steps that keep most trouble out.

The habits that keep you safe

- **Don't answer unknown numbers;** let them leave a voicemail.
- **Never give information or money to incoming contact** — always hang up and reach out yourself.
- **Use strong, unique passwords** and turn on **two-step verification** for email and banking.
- **Keep your devices updated** — updates patch the holes scammers exploit.
- **Check bank and card statements monthly** for charges you don't recognize.
- **Talk about scams with family** — the more it's discussed, the safer everyone is.

TIP

Register with the “Do Not Call” list — and know its limits

You can add your number to the national **Do Not Call Registry** (donotcall.gov) to cut down on legitimate telemarketing. Just know it won't stop *scammers* — criminals ignore the list — so it reduces the clutter but doesn't replace your vigilance. The habit of not trusting incoming calls is still your real protection.

GOOD TO KNOW

Call-blocking and spam filters help, too

Your phone can **block** numbers and silence unknown callers, and your email's spam filter catches much junk automatically. Your phone carrier may also offer free scam-call labeling. These tools quietly thin the flood of scam attempts. They're worth turning on — ask me and we'll set them up — but remember they're a helpful net, not a guarantee; the occasional scam still slips through to be handled by *you*.

CHAPTER 31

Locking Down Your Accounts and Credit

Two stronger measures deserve their own chapter, because they shut doors that scammers love to walk through: securing your logins, and freezing your credit.

Secure your key accounts

- **Turn on two-step verification** for your email, bank, and other important accounts — the single best lock, adding a texted code to your password.
- **Use a different password for each important account,** so one breach doesn't open the rest.
- **Never share a login code** that's texted to you — no real company asks you to read one back.

Freeze your credit — a powerful, free shield

A **credit freeze** blocks anyone — including a thief with your details — from opening new credit in your name. It's **free**, it doesn't affect your existing accounts or credit score, and you can lift it any time you genuinely need credit. You set it up with the three credit bureaus (Equifax, Experian, TransUnion). For most retired folks who rarely open new credit, it's a wonderful, low-effort protection.

STAY SAFE

A credit freeze is one of the best free protections there is

If identity theft worries you, a credit freeze is among the most effective steps you can take, and it costs nothing. Even if a scammer gets your Social Security number, a freeze stops them opening loans or cards in your name. It's a little bit of setup — a great thing to do together — for a great deal of peace of mind. Ask me and we'll arrange it.

FROM BILL

Let's set up your locks together

Two-step verification and a credit freeze are exactly the kind of once-done protections that are quick and painless with someone beside you, and genuinely powerful. If you'd like to spend a worthwhile half-hour making your accounts and identity much harder to touch, call me at (330) 200-8042 and we'll lock things down, step by step.

CHAPTER 32

If You Think You've Been Scammed

If a scam has gotten you or someone you love, the most important things are to act quickly and to be kind to yourself. Shame and panic help no one; calm, prompt steps limit the damage and often recover more than you'd expect.

Act on these steps, in order

1. **Stop all contact** with the scammer. Don't send more; don't “fix” it by following their next instruction.
2. **Call your bank or card company immediately** if money or account details were involved — they may stop or reverse a transfer, or watch the account.
3. **Change passwords** on affected accounts, starting with email and banking, from a safe device.
4. **If a computer was accessed,** disconnect it and have it checked.
5. **Report it** — to the FTC at reportfraud.ftc.gov, to local police, and to any impersonated company. Reporting helps you and others.
6. **Tell someone you trust** — a family member, or me. You don't have to carry this alone.

FROM BILL

Caught out? Call me first — fast help limits the harm

If you believe you've been scammed, please reach out quickly and without a shred of embarrassment — the faster we move, the more we can often stop or recover. Call me at (330) 200-8042 and we'll go through it together calmly: securing accounts, checking devices, and reporting it properly. I have helped many good, sharp people through this exact moment. You are not foolish, you are not alone, and we will get you to safe ground.

STAY SAFE

Time matters most with money transfers

If you've just sent a wire or a bank transfer, call your bank *immediately* — within minutes or hours there is sometimes a chance to stop or recall it that vanishes with time. Gift cards too: report them to the issuing store's fraud line right away, as a few have occasionally frozen unredeemed cards. Speed is everything here, so don't delay out of embarrassment — make the call now.

CHAPTER 33

Beware the “Recovery” Scam

There's one final, especially cruel trick to warn you about: the **recovery scam**, which targets people who have *already* been scammed. Knowing about it in advance protects you from being victimized twice.

How it preys on victims

After a scam, you may be contacted by someone claiming they can **recover your lost money** — a “fund recovery service,” a “government task force,” or even a “lawyer.” They ask for an upfront fee, or your bank details “to return the funds.” It's the same criminals, or their associates, coming back because they know you're a proven target and desperate to recover your loss.

SCAM ALERT

No legitimate service asks for money upfront to recover your money

Be very clear-eyed here: **anyone who contacts you promising to recover scammed money — especially for an upfront fee, in gift cards or crypto — is running a second scam.** Real authorities don't operate this way and never charge you to return your own money. If you've been scammed, work only with your actual bank and official channels (ftc.gov), and run any “recovery” offer past a trusted person first. Don't let grief make you a target twice.

FROM BILL

After a scam, let me help you sort real help from fake

The period right after being scammed is when you're most vulnerable to these follow-up tricks, because you so badly want to make it right. Please lean on trusted help instead of strangers who appear offering to fix it. Call me at (330) 200-8042 and we'll pursue the legitimate avenues together, and steer well clear of the vultures. You deserve real support, not a second wound.

CHAPTER 34

Helping a Loved One Stay Safe

Perhaps you're reading this not only for yourself but for a parent, spouse, or friend you worry about. Helping someone stay scam-safe takes a gentle touch — here's how to do it with respect and love.

How to help without hurting

- **Talk *with*, not down to.** Share scam stories as news ("did you hear about this one?") rather than lectures. No one likes to feel patronized.
- **Agree on a family safe word** for emergencies, and a habit of "let's check together" before anyone acts on an urgent call.
- **Make yourself the safe person to call** — "call me first, anytime, about anything odd, even at 2 a.m." — with genuine warmth and zero judgment.
- **Set up the protections together** — two-step verification, a credit freeze, call-blocking — as a team project, not a correction.

TIP

Make it safe to say "I think I made a mistake"

The single most protective thing a family can do is make it *emotionally safe* to admit a slip. Scams thrive on shame and secrecy; a person who fears being scolded will hide a problem until it's a disaster. Let your loved one know, often and warmly, that you'll never judge them for being targeted and that coming to you early is exactly the right thing. That openness is worth more than any gadget.

FROM BILL

I'm glad to be your family's "first call"

If you're caring for a loved one from a distance, or just want a trusted local hand, I'm honored to be the person they can call about anything that seems off — patiently, kindly, with no judgment and no rush. Sometimes just having a knowledgeable someone to check with is all it takes to keep a person safe for years. Give them my number: (330) 200-8042.

CHAPTER 34a

Watching Your Accounts and Identity

A steady habit of keeping an eye on your money and identity catches trouble early — often before a scammer can do much damage. None of it is hard; it's mostly a matter of looking now and then.

Simple monitoring habits

- **Review bank and card statements monthly** for charges you don't recognize — even small ones, which scammers use to test a stolen card.
- **Turn on transaction alerts** — your bank can text or email you when your card is used, so you spot fraud instantly.
- **Check your free credit reports** at annualcreditreport.com to catch accounts opened in your name.
- **Watch your Medicare and insurance statements** for services you never received.

TIP

Transaction alerts turn your phone into a fraud alarm

One of the easiest, most effective protections: ask your bank to turn on **alerts** that notify you each time your card or account is used. Then an unexpected charge pings your phone the moment it happens, and you can call the bank at once. It's like a little alarm on your money — free, and genuinely powerful. We can set these up together if you like.

GOOD TO KNOW

Small mystery charges are often a test — don't ignore them

If you spot a tiny charge you don't recognize — a dollar or two — don't shrug it off. Thieves often make a small “test” charge to see if a stolen card works before attempting something big. Report any charge you don't recognize to your bank, however small. Catching the test stops the real theft.

CHAPTER 34b

What Scammers Do With Your Information

It helps to understand *why* scammers want the bits of information they ask for, because it makes you rightly protective of things that might seem harmless to share.

Why these details matter

What they want	What they do with it
Your Social Security number	Used to open accounts and file fake tax returns in your name. Guard it fiercely.
Your date of birth / mother's maiden name	Common answers to security questions — keys to your accounts.
A login code texted to you	Lets a scammer walk past your two-step verification in real time.
Your Medicare / insurance number	Used to bill for fake medical services.
Account numbers	Direct access to your money.

STAY SAFE

Guard the “boring” details too

Scammers don't only want your passwords — your birthday, your first pet's name, your mother's maiden name, and other “harmless” facts are exactly the answers to security questions that protect your accounts. Be thoughtful about sharing these publicly (including on social media quizzes designed to collect them). The small, dull details are often the keys to the big doors.

FROM BILL

Worried your information is “out there”? Let's make a plan

If you fear your details may have been exposed — in a scam, or one of the big company data breaches you hear about — don't lose sleep; make a plan. We can freeze your credit, tighten your accounts, and set up monitoring so you're protected going forward. Call (330) 200-8042 and we'll turn worry into a concrete, calming set of steps.

CHAPTER 34c

Scam-Proofing Your Phone and Devices

A few settings on your phone and computer quietly block a lot of scam attempts before they ever reach you. Think of this as a final once-over of your defenses.

Settings worth turning on

- **Silence or block unknown callers** so scam calls go to voicemail.
- **Turn on spam filtering** for texts and email.
- **Enable two-step verification** on email, banking, and key accounts.
- **Keep automatic updates on** so security holes get patched.
- **Set a screen lock** (passcode, Face ID, or fingerprint) so a lost phone stays shut.

TIP

A once-done setup pays off for years

These settings take an afternoon to turn on and then protect you quietly for years. It's the best kind of security — set once, working forever in the background, asking nothing more of you. If sorting through the menus feels daunting, this is a perfect thing to do together: we'll switch on every protective setting in one sitting.

FROM BILL

Let's give your devices a safety once-over

I love doing a “safety once-over” with folks — we go through the phone and computer together and switch on every protective setting: call blocking, spam filters, two-step verification, updates, a screen lock. You walk away knowing your devices are set up to help keep you safe, not leave you exposed. Call (330) 200-8042 and we'll make it happen.

WHAT THIS DOES FOR YOU

You are now a hard target — and that's the whole point

Put it all together — the red flags you can spot, the golden rules you follow, the settings you've switched on, the trusted people you'll call — and you've become exactly what scammers dread: alert, unhurried, protected, and connected. They thrive on the opposite of all those. You've turned yourself from an easy mark into a dead end for them. Be proud of that.

CHAPTER 34d

The Emotional Side of Being Scammed

If a scam has gotten you, the hardest part is often not the money — it's the feelings: shame, embarrassment, anger at yourself, a shaken sense of trust. I want to speak to that directly, with kindness, because how you treat yourself afterward matters a great deal.

Please be gentle with yourself

Being scammed is not a character flaw or a sign of decline. It means a professional criminal, whose entire job is manipulation, caught you in a vulnerable moment — as they do to millions of capable, intelligent people every year, of every age. The shame belongs entirely to *them*, not to you. You were the victim of a crime, no different from someone whose pocket was picked.

FROM BILL

I have never once judged someone who was scammed — and I never will

In all my years, I've sat with many good people in the hours after a scam, and I can tell you honestly: not once have I thought less of a single one of them. What I've felt is anger at the crooks and admiration for the courage it takes to reach out and set things right. If this has happened to you, please call me — (330) 200-8042 — and know you'll be met with nothing but help and respect.

Don't let shame make it worse

The cruelest thing shame does is keep people silent — so they don't report it, don't warn their family, and become targets for the “recovery” scammers who prey on that isolation. Breaking the silence is how you take your power back. Tell someone you trust. Report it. You'll feel lighter, and you'll help protect others.

WHAT THIS DOES FOR YOU

Turning a hard experience into strength

Here's the hopeful truth: people who've been through a scam and talked about it openly often become the *safest* people of all — and wise protectors of their friends and family. A hard experience, faced honestly, becomes hard-won wisdom. If it's happened to you, you are not diminished; you're now someone who truly understands, and that understanding can keep many people safe.

CHAPTER 34e

Talking With Grandchildren and Family About Scams

Scam safety isn't only for older adults — younger people get caught too, often by different scams (fake job offers, online shopping, social media). Making scams a comfortable family topic protects everyone and strengthens the bonds that keep you all safe.

Making it a family conversation

- **Share stories, not lectures** — “look at this clever scam I read about” invites everyone in without anyone feeling talked-down-to.
- **Set up a family safe word** together, for emergency-call scams.
- **Agree you'll all “check with each other”** before acting on anything urgent and money-related.
- **Learn from the young folks too** — grandchildren often know the newest tricks, and love being asked.

TIP

A family that talks about scams is a family that's hard to scam

The single most protective thing a family can build is an easy, open habit of talking about scams — swapping the latest tricks, agreeing to check with one another, never judging a near-miss. Scammers isolate; families connect. When everyone from the grandchildren to the grandparents is in the habit of saying “hey, is this a scam?”, the whole family becomes a fortress.

WHAT THIS DOES FOR YOU

Safety and closeness, hand in hand

There's a lovely bonus in all this: the very habits that keep your family safe from scams — checking in with each other, sharing what you've learned, being the trusted person someone can call — also bring you closer together. Protecting one another is an act of love. In guarding against the scammers, you end up a little more connected to the people who matter most. That's a fine thing to come out of all this.

PART 8

When to Call Bill & Your Cheat-Sheet

An honest word about leaning on a trusted hand — and a one-page cheat-sheet of the red flags and golden rules to keep right by your phone.

CHAPTER 35

When to Call Bill

This book is here to make you confident and hard to fool. But the smartest, safest people aren't the ones who never ask for help — they're the ones who check with someone they trust whenever something feels off. So here's when I'd want you to pick up the phone.

Call me — anytime — when

- **Anything gives you that "this doesn't feel right" twinge.** Trust it. That's exactly what I'm here for.
- **You got a call, message, or pop-up** you're not sure about, and you'd like a second set of eyes before you act.
- **You think you may have been scammed** — call quickly, and without any shame.
- **You let someone onto your computer** or shared information you shouldn't have.
- **You'd like to set up protections** — two-step verification, a credit freeze, call-blocking, a family safe word.
- **You're worried about a loved one** and want help keeping them safe.

FROM BILL

How I like to help

I'm Bill, and I've spent 30+ years helping folks feel at home and safe with their technology, right here in Portage County, Ohio. I don't rush, I don't talk down to anyone, and there is truly no such thing as a silly question at my table — least of all about scams. Whether it's a two-minute "is this real?" call or sitting down to lock everything tight, we'll handle it together. Call **(330) 200-8042** or book a time at **billshometech.com/book**.

STAY SAFE

There is never any shame in asking — only wisdom

If you take one feeling from this whole book, let it be this: checking with someone before you act is not weakness or foolishness — it is exactly what careful, intelligent people do. Scammers win in isolation and lose in conversation. Every time you pause to ask, you rob them of their one advantage. So ask freely, ask often, and never once feel small for it.

Thank you for taking the time to learn this. You are now far harder to fool than you were a few hours ago — calmer, wiser, and ready. Keep this book by the phone, trust your instincts, and remember that a quick call to someone you trust beats any scammer alive. Be proud of

yourself, and don't be a stranger.

— Bill

CHAPTER 36

Your Scam-Safety Cheat-Sheet

Copy this onto a card and keep it right by your phone and computer. In the heat of a scammer's call, one glance here can save you.

The 7 red flags — any ONE means STOP

- Pressure to act **immediately**.
- A request for **secrecy** (“don't tell anyone”).
- Payment by **gift card, wire, crypto, or payment app**.
- A request for **passwords, codes, or personal information**.
- **Contact you didn't start** (surprise call/text/email/pop-up).
- An offer **too good to be true**.
- They won't let you **hang up and verify** independently.

Bill's golden rules

- **Slow down** — no honest matter needs action in minutes.
- **Hang up and call back** on a number YOU look up.
- **Never** pay in gift cards, wire, or crypto to incoming contact.
- **Never** give passwords, codes, or computer access.
- **Talk to someone you trust** before acting.
- **When in doubt, do nothing yet.**

The lines that are ALWAYS scams

If you hear…	It's…
“Pay with gift cards.”	Always a scam. No exceptions.
“We're tech support; let us into your computer.”	Always a scam.
“Move your money to a safe account.”	Always a scam — your bank never says this.
“Your SSN is suspended / warrant for arrest.”	Always a scam — agencies don't call like this.
“You won! Just pay a fee first.”	Always a scam.

If you hear…	It's…
"I can recover your lost money for a fee."	Always a scam.

Report scams to

- **FTC:** reportfraud.ftc.gov
- **Your bank / card company** (number on your card) — right away if money was involved.
- **Local police**, and the real company that was impersonated.
- **Bill's Home Tech:** (330) 200-8042 — anytime something feels off.

WHAT THIS DOES FOR YOU

You see them coming now

Look how far you've come. You know the tricks, the red flags, the golden rules, and exactly what to do if one ever slips through. You are no longer an easy target — you're the calm, informed person scammers can't rush and can't fool. Keep this card close, trust your gut, and walk through the world with confidence. You've earned it.

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