

STAYING SAFE & CONNECTED

A Digital Guide for Older Adults

A Digital Literacy Companion Book

First Edition
Anaheim, California

Copyright © 2026 Nana Sarfo Brobbey /
Brobb's Connect. All rights reserved. First
Edition.

No part of this book may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without prior written permission from the author, except for brief quotations in a review, and except for the checklists, worksheets, and note pages, which are intended to be written in by the individual reader who owns this copy.

This book is intended for general educational purposes only. It does not constitute legal, financial, medical, or professional advice. Scam tactics, technology platforms, and program names change over time; readers should verify current details (phone numbers, websites, and procedures) before relying on them, especially in the Emergency & Important Contacts and Community Resources sections.

This book is a companion to the NAVIGATE program, a Brobb's Connect community initiative. Learn more at <https://brobbsconnect.dev>.

Table of Contents

How to Use This Book.....	9
Preface.....	11
Not Sure Where to Start? Start Here.....	12
Chapter 1: Introduction.....	13
A Different Kind of Change.....	13
Why This Matters Now.....	14
What Confidence Actually Looks Like.....	15
Where Do You Stand Today?.....	16
The Numbers Behind This Book.....	17
You Are Not as Far Behind as It May Feel.....	18
What This Book Won't Do.....	19
A Note on Pace and Patience.....	19
How This Book Is Organized.....	20
A Short History Worth Knowing.....	21
The People Behind the Curtain.....	22
Chapter 2: Getting Comfortable with Your Devices.....	24
Know Your Device.....	24
The Home Screen, Explained.....	26
A Glossary You Can Actually Use.....	26
Why Updates Matter.....	27
Storage, Batteries, and Everyday Care.....	28

A Note on Passkeys.....	29
Setting Up Medical ID on Your Lock Screen.....	29
Touchscreens: The Gestures Behind the Glass.....	31
Voice Assistants and Accessibility Features.....	32
Choosing a Device That Fits You.....	33
Understanding Notifications and Permissions.....	34
Backing Up Your Photos and Information.....	35
Chapter 3: Understanding the Internet & Email.....	37
How Browsing Works.....	37
Search Engines and How They Choose Results.....	38
Email Basics.....	39
The Habits That Keep You Safe.....	40
Blocking Robocalls and Spam Texts.....	41
Subscription Traps and Free Trial Tricks.....	43
Public Wi-Fi: What's Actually Safe.....	44
Understanding File Attachments.....	45
Choosing Safe Apps.....	46
Recognizing Fake Online Reviews.....	47
Organizing Your Digital Life.....	47
Chapter 4: Recognizing Scams & Fraud.....	49
The Architecture of a Scam.....	49
Common Scam Categories.....	50
The Psychology Behind Why It Works.....	54
Common Myths About Scams.....	55
Red Flags Worth Memorizing.....	56
A Closer Look: The Investment and Cryptocurrency Scam	57
A Closer Look: The Overpayment Scam.....	58
The Sandwich Generation and Shared Vigilance.....	59

What the Numbers Say About Each Scam Type.....	60
Grief and Holiday Scams.....	61
Charity Scams After a Disaster.....	61
Chapter 5: AI, Deepfakes & Romance Scams.....	64
What a Deepfake Actually Is.....	64
The Voice Cloning Scam.....	65
Recognizing AI-Generated Images and Video.....	66
Romance Scams.....	67
How AI Tools Are Changing Everyday Scams.....	70
Fake Websites and Storefronts.....	71
Fake Customer Service and AI Chatbots.....	72
Staying Grounded as Technology Changes.....	73
A Conversation Worth Having with Family.....	74
Chapter 6: Banking & Financial Safety Online.....	75
Getting Comfortable with Your Bank's App or Website....	75
Passwords That Actually Protect You.....	76
Two-Factor Authentication, Explained Simply.....	77
Recognizing Financial Fraud in Progress.....	78
Your Rights as a Banking Customer.....	79
Checking Your Accounts Regularly.....	80
Understanding How Money Actually Moves.....	80
How to Dispute a Charge.....	81
Verifying a Financial Advisor.....	82
Credit Freezes and Fraud Alerts.....	83
Financial Exploitation by Someone You Know.....	83
Chapter 7: Healthcare Systems Online.....	87
Understanding Patient Portals.....	87
Telehealth Visits.....	88

Protecting Your Health Information.....	89
Reviewing Your Explanation of Benefits.....	90
Understanding Your Rights Under HIPAA.....	90
Choosing a Care Proxy or Medical Power of Attorney.....	91
Shopping for Hearing Aids Without Getting Scammed....	92
Mental Health Support Through Telehealth.....	93
Chapter 8: Government Services Online.....	96
The Golden Rule of Government Contact.....	96
Setting Up my Social Security Account.....	97
Medicare Online.....	98
Filing Taxes and Avoiding IRS Scams.....	98
Choosing a Tax Preparer, You Can Trust.....	99
Medicare Open Enrollment: A High-Risk Season.....	101
Renewing Licenses and Other State Services.....	102
Understanding Benefit Statements and Notices.....	103
The Difference Between Medicare Parts.....	103
Saving Money on Prescriptions.....	104
Chapter 9: Community Resources & Local Support.....	107
Your Local Library.....	107
Senior Centers.....	108
Researching Assisted Living and Aged Care Options.....	109
Transportation Help.....	110
Food and Meal Support.....	110
Planning for Your Digital Legacy.....	111
Faith Communities and Civic Organizations.....	113
Home Safety and Fall Prevention Resources.....	113
Smart Speakers and Voice-Activated Help at Home.....	115
Continuing Education and Lifelong Learning.....	116

Volunteering and Giving Back.....	117
Getting Help with Errands and Household Tasks.....	117
A Note for Adult Children and Caregivers.....	119
Chapter 10: Social Media & Staying Connected Safely.....	121
Privacy Settings, Explained.....	121
What Not to Share, and Why.....	122
Understanding Algorithms and Your Feed.....	123
Marketplace and Buy-Sell Groups.....	124
Sharing Photos Across the Family.....	125
Recognizing Online Harassment.....	126
Texting Like the Rest of the Family.....	127
Staying Connected Through Video Calls.....	128
Chapter 11: Building Your Digital Confidence Score.....	130
The Full Self-Assessment.....	130
Why Scoring Yourself Honestly Matters.....	132
Understanding Score Plateaus.....	132
Measuring Progress Together.....	133
A 30-Day Practice Plan.....	134
Setting Goals for What's Left.....	135
Immediate Steps.....	136
Reporting the Scam.....	137
Filing a Local Police Report.....	138
If Personal Information Was Exposed.....	139
Should You Pay for Identity Theft Protection?.....	140
Emotional Recovery Matters Too.....	141
Helping Someone Else Who Has Been Scammed.....	142
What Recovery Actually Looks Like Over Time.....	142
Chapter 13: Emergency & Important Contacts.....	145

Emergencies.....	145
Fraud & Scam Reporting.....	146
Financial.....	146
Government.....	147
Community & Aging Services.....	147
My Personal Contacts.....	148
Chapter 14: Quick-Reference Appendix.....	149
Glossary.....	149
Frequently Asked Questions (FAQs).....	150
The Red Flags Checklist (Tear-Out).....	151
Troubleshooting FAQ.....	151
Finding Help in Your State.....	152
What's Changed Since This Book Was Printed.....	153
About the Author.....	154
About Brobbs Connect & NAVIGATE.....	155
Acknowledgments.....	156
Tell Us Your Story.....	159
Notes.....	160
Notes.....	161
Notes.....	162

How to Use This Book

This book is meant to be used, not just read. You will see a few recurring features throughout each chapter, designed to help the ideas stick and give you something to practice, not just remember.

TRY IT YOURSELF

A short, guided activity to do right on your own device as you read. No rush, no wrong answers.

SPOT THE SCAM

A real-looking example message, call, or website for you to examine and decide: is this legitimate, or a scam? The answer follows.

TALK ABOUT IT

A conversation starter to bring up with family, friends, or your NAVIGATE group.

CHECKLIST

A short self-check to see where you stand before moving on.

MY NOTES

Blank space for your own thoughts, questions, or reminders. Write in this book. It's yours.

You do not have to read this book cover to cover in one sitting. Many readers work through one chapter a week alongside their NAVIGATE sessions. Go at your own pace. That is the whole point.

Preface

I grew up in Ghana, in a family and a community where looking after older relatives was never treated as optional. It was simply what you did. When I moved to the United States and settled in Southern California, I began spending time in community spaces where I saw a different, quieter problem: older adults who were capable, sharp, and independent in every other part of their lives, but who felt shut out of a world that had moved almost entirely online.

I watched people lose money to callers pretending to be their grandchildren. I watched others avoid online banking altogether out of fear, even when it would have made their lives easier. And I watched how much confidence came back once someone simply sat down and explained things clearly, without judgment and without rushing.

That is what NAVIGATE was built to do, and it is what this book is for. It is not a book about becoming a technology expert. It is a book about staying safe, staying connected to the people and systems that matter and feeling confident enough to ask questions without embarrassment.

I hope you keep this book close, write in its margins and come back to it whenever you need to.

Not Sure Where to Start? Start Here

This book is designed to be read in order, but if something specific is worrying you right now, it's fine to jump straight to the chapter that addresses it and come back to the rest later.

"I got a scary phone call and I'm not sure what to do." Go to Chapter 4 (Recognizing Scams & Fraud) and Chapter 12 (What to Do If You've Been Scammed).

"I want to feel safer banking online." Go to Chapter 6 (Banking & Financial Safety Online).

"I'm worried about a family member's new online relationship." Go to Chapter 5 (AI, Deepfakes & Romance Scams).

"I just want to feel more comfortable with my phone or tablet." Go to Chapter 2 (Getting Comfortable with Your Devices).

"I need help finding local resources near me." Go to Chapter 9 (Community Resources & Local Support).

"Something already happened and I need help right now." Go straight to Chapter 13 (Emergency & Important Contacts).

Wherever you start, this book will still be here for everything else when you're ready for it.

Chapter 1: Introduction

If you are reading this, you have probably already noticed that the world has quietly moved online. Doctor's appointments, bank statements, family photos, even conversations with grandchildren: a large share of daily life now happens through a screen. That shift can feel exciting. It can also feel like it happened without asking your permission.

This book will not try to turn you into a computer expert. It has one goal: to help you use technology confidently and safely, on your own terms, at your own pace.

A Different Kind of Change

Think for a moment about how many times the tools of daily life have changed over the course of your lifetime. Rotary phones gave way to touch-tone, then to cordless phones, then to mobile phones, then to the smartphones many of us now carry everywhere. Typewriters became word processors became laptops. Paper checks and passbooks became debit cards, and now many transactions happen with a tap or a glance.

Every one of those changes asked something of the people living through it. What feels

different about the current shift is speed. Earlier technologies tended to arrive one at a time, with years between them to adjust. Today, a bank might redesign its website, a phone might push a software update, and a new scam technique might appear, all in the same month. It is not that you are falling behind. It is that the ground keeps moving faster than any one person could reasonably be expected to track alone.

That is precisely why a program like NAVIGATE, and this book alongside it, exists: not to make you chase every change, but to give you a stable set of principles and habits that hold up no matter what specific app or scam happens to be popular this year.

Why This Matters Now

Older adults are targeted by scammers more than almost any other group, not because they are less capable, but because scammers assume they will be less likely to report it, more likely to be polite to a stranger on the phone, and less familiar with how fast technology changes. That assumption is exactly what this book is here to break.

Consider how a typical scam call is built. It relies on three things: catching you off guard, creating urgency, and exploiting trust in an

institution or a family relationship. A caller claiming to be from Medicare, or a grandchild claiming to be in trouble, is counting on you reacting quickly and emotionally rather than pausing to verify. Every chapter in this book, especially Chapters 4 and 5, is designed to give you the pause button that scam artists are counting on you not having.

At the same time, the systems you rely on, including Social Security, Medicare, your bank, and your pharmacy, increasingly expect you to interact with them online. Avoiding technology entirely is no longer a safe option either, since paper processes are often slower, and some services now function best, or only, through a website or app. The goal of this book is not to avoid the digital world. It is to move through it with your eyes open, so that convenience and safety work together rather than against each other.

What Confidence Actually Looks Like

It is worth pausing on what “digital confidence” really means, because it is often misunderstood. Confidence does not mean knowing every button on every app. It does not mean never feeling confused. Even people who have used computers professionally for

decades regularly encounter something new and must slow down and figure it out.

Real confidence looks like this: knowing that when something feels off, whether it's an unexpected phone call, a strange email, or a website that looks slightly wrong, you have a reliable process for slowing down, checking, and deciding what to do next. It looks like being willing to ask a question rather than guessing and hoping for the best. And it looks like understanding that mistakes online are usually fixable, especially if you catch them early and know who to call.

This book is built around that kind of confidence. Every chapter gives you both the background knowledge and the specific, practiced habit that turns knowledge into instinct.

Where Do You Stand Today?

Before we go further, take a moment to be honest with yourself about where you're starting from. There are no wrong answers here, and this is not a test with a passing score. It is simply a snapshot, so that later in the book, in Chapter 10, you can look back and see how far you have come.

CHECKLIST Where Do You Stand Today?

- ☐ I feel confident sending and reading email.
- ☐ I know what two-factor authentication is.
- ☐ I could explain to a friend how to spot a scam text message.
- ☐ I know who to call if I think I've been scammed.
- ☐ I use the internet to manage my healthcare or benefits.
- ☐ I feel confident, not anxious, when I get an unexpected call or email.

Count how many boxes you checked. That number is your starting Digital Confidence Score. We will come back to this exact list in Chapter 10, after you've worked through the book, so you can see how much has changed. You may be surprised to find you already knew more than you gave yourself credit for, or you may find real, specific gaps you can now name and close. Both outcomes are useful.

TALK ABOUT IT

Share your checklist results with a family member or your NAVIGATE group. Ask them: which of these would you check for yourself?

The Numbers Behind This Book

It can help to see the scale of what this book addresses in plain numbers, drawn from federal sources. The Federal Trade Commission's most recent report to Congress found that total fraud losses reported by adults 60 and older roughly quadrupled between 2020 and 2024, rising from about 600 million dollars to 2.4 billion dollars in a single year, and the FTC believes the true figure, including unreported losses, is likely many times higher. The FBI's Internet Crime Complaint Center separately reported that Americans 60 and older lost close to 7.7 billion dollars in 2025 alone, a jump of nearly 60 percent over the year before.

A few specific figures are worth sitting with. Older adults who lose money to a scam tend to lose far more per incident than younger victims, with median losses for people 80 and older exceeding 1,600 dollars, more than any other age group. Investment scams, often beginning on social media, have become the single largest loss category. And fraud connected to artificial intelligence, including the voice cloning covered in Chapter 5, accounted for hundreds of millions of dollars in reported losses in 2025 alone, a category

that essentially did not exist in its current form just a few years earlier.

None of this is presented to frighten you. It's presented because the scale of the problem is precisely why a book like this exists, and precisely why the habits in the coming chapters are worth taking seriously rather than treating as an abundance of caution. You are not imagining the scope of this threat, and you are not overreacting by taking it seriously.

You Are Not as Far Behind as It May Feel

It is also worth knowing, in plain numbers, that older adults have been closing the technology gap faster than most people assume. Recent national research from the Pew Research Center found that 91 percent of adults 50 and older now own a smartphone, up from just over half a decade ago, and roughly 9 in 10 adults 65 and older now use the internet in some form. Nearly all older adults surveyed by AARP said they rely on technology specifically to stay connected with family and friends, which is precisely the goal this book is built to support safely.

If you sometimes feel behind or feel that everyone else finds this easier than you do, the data suggests otherwise: an enormous

number of your peers were exactly where you are now within the past several years, and have since become comfortable, capable users of the same tools this book covers.

What This Book Won't Do

It's worth being honest about the limits of a book like this one, since overpromising helps no one. This book cannot make you immune to every future scam, since tactics will keep evolving after these pages are printed, as covered throughout Chapter 5. It cannot replace a hands-on class, a patient family member, or your own repeated practice; reading about turning on two-factor authentication is not the same as doing it. And it cannot remove the genuine effort required to build new habits later in life, effort that is real but, as the data in this chapter shows, entirely achievable.

What it can do is give you a reliable foundation, a shared vocabulary with the NAVIGATE program and with your family, and a reference to return to whenever something new and unfamiliar shows up. That is a realistic, worthwhile goal, and it's the one this book is built to meet.

A Note on Pace and Patience

There is a temptation, especially with a book like this, to feel you should already know most of it. Set that feeling aside if you can. The people who eventually feel most confident with technology are rarely the ones who moved fastest. They are the ones who kept showing up, asked questions without embarrassment, and let understanding build slowly, one habit at a time.

You are also not doing this alone. This book exists alongside the in-person NAVIGATE program, where you can ask questions in real time, alongside other adults working through the same material. If something in this book does not make sense on the page, that is exactly the kind of question worth bringing to a session.

How This Book Is Organized

Each chapter builds on the last, moving from the basics of your devices to the internet and email to recognizing scams, to specific systems like banking, healthcare, and government services. Chapter 9 turns outward to the community resources around you, from libraries to senior centers to transportation help, because staying safe online is only part of navigating daily life well. The book closes with a full emergency

contacts section and a quick-reference appendix you can keep handy by the phone or in your bag.

You do not need to read this book in one sitting, and you do not need to read it alone. NAVIGATE participants may work through one chapter a week, alongside the program's sessions, returning to earlier chapters as questions come up in daily life. Treat this book less like a textbook to finish and more like a reference you will return to for years.

A Short History Worth Knowing

It can help to understand that the anxiety many people feel about new technology is not a personal shortcoming, it is a completely ordinary human response to unfamiliar tools, and it has happened before. When automatic teller machines first appeared in the 1970s, banks ran extensive newspaper advertising specifically to reassure customers that using one did not require any special skill, and many older customers at the time avoided them for years, preferring the teller window, before eventually adopting them as the norm. The same pattern repeated with online banking in the late 1990s, with smartphones in the following decade, and it is repeating again now with AI-powered tools. Every generation

faces a version of this same adjustment. What has changed is only the specific technology being adjusted to, not the underlying human experience of learning something new later in life.

This history matters because it reframes what you are doing as you read this book. You are not behind. You are doing something every generation before yours has also had to do; catching up to a tool that arrived faster than anyone was consulted about.

The People Behind the Curtain

It also helps to understand who, specifically, is on the other end of a scam attempt, because it demystifies something that can otherwise feel abstract and frightening. Law enforcement investigations, including reporting from the FBI and international partners, have traced large volumes of scam activity targeting American seniors to organized operations, some run out of call centers overseas, others run domestically, that treat fraud as a business with scripts, quotas, and management structures much like any other sales operation, except the product being sold is a lie.

This is worth knowing for two reasons. First, it explains why scam attempts often feel so

polished and rehearsed: the person on the phone may have made the same call, with the same script, dozens of times that day. Second, it should remove any lingering sense that falling for a well-run scam reflects poorly on you personally. A trained salesperson working from a tested script, aimed specifically at bypassing your defenses, is a formidable opponent. The goal of this book is not to make you immune to every conceivable tactic. It is to give you the specific, practiced habits that stop most of these attempts before they succeed.

MY NOTES

Chapter 2: Getting Comfortable with Your Devices

Every device you own, whether it's a smartphone, a tablet, or a desktop computer, is built around a small set of ideas that repeat over and over. Once those ideas feel familiar, a new app or a new screen stops feeling frightening and starts feeling like something you can figure out.

It helps to remember that every person who now uses a smartphone comfortably, including your grandchildren, was once a beginner too. Nobody is born knowing what a gray gear-shaped icon means. They learned it by seeing it, tapping it, and noticing what happened. You can learn the same way, and this chapter is built to give you that same repeated, low-stakes exposure.

Know Your Device

Take a moment to identify what you own. Many people use words like “iPad” or “phone” loosely without knowing which operating system it runs, and that matters because instructions differ between them. Broadly, devices fall into two families. Apple devices, including the iPhone and iPad, run a system

called iOS or iPadOS. Most other phones and tablets, made by companies like Samsung, Google, and others, run a system called Android. Windows and Mac are the two main systems for desktop and laptop computers.

Knowing which family your device belongs to matters because when you search for help online, or ask a family member a question, the answer often depends on it. “How do I turn off notifications on my iPhone” and “how do I turn off notifications on my Android phone” have different answers, even though the goal is the same.

TRY IT YOURSELF Label Your Own Device

Get the device you use most and find these on it right now:

1. The power button (usually on the side or top edge).
2. The volume buttons.
3. The home screen or main screen.
4. The settings icon (often looks like a gray gear).
5. The camera icon.

Write down where each one is located, in your own words, in the notes box below.

MY NOTES

The Home Screen, Explained

Your home screen is simply a collection of shortcuts. Each small picture, called an icon, is a doorway into one app. Tapping it opens that app; nothing more complicated is happening underneath. If you tap the wrong one, you have not broken anything. You can always press the home button or swipe up from the bottom of the screen depending on your device, to return to the home screen and try again.

This is worth repeating because so much anxiety around technology comes from a fear of “breaking” something. Modern devices are built to be very difficult to break through ordinary use. Tapping an unfamiliar icon, opening a menu you don’t recognize, or pressing a button you’re unsure about will almost never cause permanent harm. The habits in this book are about safety from

scams and fraud, not about being afraid of the device itself.

A Glossary You Can Actually Use

New technology comes with new words, and unfamiliar vocabulary is one of the biggest reasons people feel shut out. Here are the terms you'll see most often in this book and in daily life. Treat this page like a set of flashcards; come back to it whenever a term feels unfamiliar, and don't feel you need to memorize it all at once.

App (application): a program you open on your phone or tablet to do something specific, like check the weather or send a message.

Browser: the app you use to visit websites, such as Safari, Chrome, or Edge.

Cloud: a way of storing your photos and files on the internet instead of only on your device, so you can reach them from anywhere.

Notification: a small alert that pops up on your screen to tell you something happened, like a new message.

Password manager: a tool built into your device or browser that remembers your passwords for you, so you don't have to.

Update: a fix or improvement that a company sends to your device. Updates often close

security gaps, so they matter more than they might seem to.

Wi-Fi: a wireless way to connect your device to the internet, usually at home or in a public place like a library.

Why Updates Matter

It is tempting to dismiss update reminders, especially when they interrupt something you're doing. It helps to understand what an update is. Software companies employ teams of people whose job is to look for weaknesses in their own systems before criminals find them first. When a weakness is discovered, the company builds a fix and sends it to your device as an update. Delaying an update means leaving that weakness open longer than necessary.

This does not mean every update needs to happen the instant it appears. It does mean checking every so often, ideally monthly, and not indefinitely postponing updates out of habit. Most devices can also be set to update automatically overnight, which removes the decision from your hands entirely.

TRY IT YOURSELF Check for Updates

On an iPhone or iPad: open Settings, then

General, then Software Update.

On an Android device: open Settings, then System, then System Update (menu names vary slightly by manufacturer).

On a Windows computer: open Settings, then Windows Update.

On a Mac: open System Settings, then General, then Software Update.

If an update is available, note the date, and consider installing it while your device is plugged in and you have time to wait.

Storage, Batteries, and Everyday Care

A few practical habits keep your device running well and reduce frustration. Charge your device overnight rather than letting the battery run all the way to zero regularly. Restart your phone or computer every few days; this clears small errors that build up during normal use. If your device runs slowly, check how much storage space remains, since a nearly full device often slows down; deleting unused apps or old photos you've already backed up can help.

None of this needs to be memorized perfectly. The point is simply to know that these options exist, so that when something feels slow or

wrong, you have a starting place rather than a feeling of helplessness.

A Note on Passkeys

You may start noticing an option called a “passkey” when logging into accounts, offered as an alternative to typing a password. A passkey uses your device’s own fingerprint, face recognition, or screen lock instead of a typed password, and is generally considered more secure, since there’s no password for a scammer to steal through a phishing message in the first place. Setting one up is optional wherever it’s offered, and your existing password continues to work alongside it, so there’s no pressure to switch before you feel ready. If a screen ever offers to set up a passkey for an account you use often, it’s a reasonable, low-risk option to accept.

Setting Up Medical ID on Your Lock Screen

Both iPhones and Android phones let you store basic medical information, such as allergies, medications, and an emergency contact, in a way that’s visible from the locked screen without requiring a passcode, specifically so first responders can access it in an emergency even if you’re unable to unlock

your phone yourself. This is a small, one-time setup that can matter enormously in exactly the kind of moment covered in Chapter 9's discussion of falls and medical emergencies.

TRY IT YOURSELF Set Up Your Medical ID

On an iPhone: open the health app, tap your profile picture, then Medical ID, then Edit, and fill in your information. Make sure "Show When Locked" is turned on.

On an Android device: open Settings, then Safety & Emergency (menu names vary slightly by manufacturer), and fill in your medical information and emergency contacts.

Ask a family member to help you fill this in if any of it feels uncertain to enter alone.

CHECKLIST Device Basics Check

- ☐ I know whether my phone or tablet is an iPhone/iPad (Apple) or Android.
- ☐ I know how to turn my device's volume up and down.
- ☐ I know where the settings app is.
- ☐ I know how to check if my device needs an update.
- ☐ I know how to lock my screen with a passcode.

Touchscreens: The Gestures Behind the Glass

Touchscreens communicate through a small vocabulary of gestures, and once you know them, nearly every app behaves in roughly the same way. A single tap opens something. A press and hold, sometimes called a long press, usually reveals additional options, like the ability to delete or move an icon. Swiping, dragging a finger across the screen, scrolls through a list or moves between screens. Pinching two fingers together or spreading them apart zooms out or in on a photo or webpage.

These gestures are consistent across many apps, which is precisely what makes a touchscreen device, once its basic vocabulary is learned, genuinely easier to use long term than the layered menu systems of older computers. A new app rarely requires learning an entirely new way of interacting; it almost always reuses this same small set of gestures in a new arrangement.

TRY IT YOURSELF Practice the Core Gestures

Open your Photos app and try each gesture on a photo:

1. Tap once to open it fully.
2. Pinch two fingers together, then spread them apart, to zoom out and in.
3. Swipe left or right to move to the next photo.
4. Press and hold on a photo to see what extra options appear.

Voice Assistants and Accessibility Features

Most modern devices include a built-in voice assistant, such as Siri on Apple devices or Google Assistant on Android, that can perform many tasks entirely by spoken command: setting a reminder, reading a text message aloud, or calling a contact by name without touching the screen at all. For anyone who finds small text or precise tapping difficult, this can be a genuinely useful alternative path into the same tasks covered elsewhere in this book.

Beyond voice assistants, every modern device includes a dedicated accessibility menu, built specifically to make the device easier to see, hear, and operate. This includes text size adjustment, which can make every app on the device display larger text without needing each individual app to be changed separately, high-contrast display modes, and options to

slow down or simplify on-screen animations that some people find disorienting.

TRY IT YOURSELF Adjust Your Text Size

On an iPhone or iPad: Settings, then Accessibility, then Display & Text Size, then Larger Text.

On an Android device: Settings, then Accessibility, then Font Size (menu names vary slightly by manufacturer).

Try increasing the size by one or two steps and see how it feels across a few different apps.

Choosing a Device That Fits You

If you're shopping for a new phone, tablet, or computer, it's worth knowing that your choices generally fall into three categories, each suited to a different comfort level, rather than assuming you must buy whatever is most popular or most advertised. Understanding the category helps far more than chasing a specific brand name.

Mainstream tablets and phones, like a standard iPad, Samsung Galaxy tablet, or Amazon Fire tablet, offer the widest range of apps and the accessibility settings covered throughout this chapter, and work well for anyone reasonably comfortable following the

activities in this book. A second category, sometimes called simplified or senior-specific devices, trades away some flexibility for a dramatically easier starting point: a locked-down set of large icons for calling, video chatting, and photos, often with a family member able to preload contacts and manage settings remotely through a companion app, and typically sold with an ongoing monthly service fee alongside the device cost. These can be a genuinely good fit for someone who wants to stay connected to family without navigating an open, unrestricted device, though the added monthly cost is worth weighing against a standard tablet paired with the accessibility settings already built into it for free.

A third option worth knowing about, if a full tablet feels like more than you need, is a simplified cell phone built specifically for voice calls and texting with minimal extra complexity, still offering an emergency button and larger, physical or high-contrast buttons. Whichever category fits you best, it's worth trying a device in person at a store, when possible, since screen size, button size, and overall weight all affect day-to-day comfort in ways a photo or review can't fully convey.

Understanding Notifications and Permissions

When you first open a new app, it will often ask permission to do something specific: use your camera, know your location, or send you notifications. These requests exist because of privacy rules that require apps to ask before accessing sensitive information, rather than simply taking it. It is worth reading each request rather than tapping through automatically, and it is always safe to say no to a permission that doesn't make sense for what the app does. A simple calculator app, for instance, has no legitimate reason to need access to your contacts or location.

Notifications, the small alerts and sounds an app sends you, can be adjusted or turned off entirely for any app that sends too many. This is found in the same Settings area as text size, typically under "Notifications," where each app can be individually managed. Reducing notifications from apps you don't check often is a simple way to make your device feel calmer and less overwhelming.

Backing Up Your Photos and Information

One of the quieter benefits of modern devices is automatic backup: many phones and tablets

can be set to automatically copy your photos, contacts, and other information to the cloud, the internet-based storage mentioned earlier in this chapter, so that if your device is ever lost, stolen, or damaged, nothing is permanently gone. This is worth setting up once and then largely forgetting about, since it runs quietly in the background.

TRY IT YOURSELF Check If Your Photos Are Backing Up

On an iPhone: Settings, tap your name at the top, then iCloud, then Photos, and confirm “iCloud Photos” is turned on.

On an Android device: open the Photos app, tap your profile picture, and check that Backup is turned on.

If it’s off, turn it on and connect to Wi-Fi to let your existing photos back up.

TALK ABOUT IT

Ask a family member to show you one setting on your device you’ve never used before. Write down what you learned.

MY NOTES



Chapter 3: Understanding the Internet & Email

The internet can feel like an enormous, invisible place. In practice, almost everything you do online falls into a small number of categories: browsing websites, sending email, and using apps. This chapter focuses on the first two, since they are the foundation for nearly everything else in this book.

It helps to think of the internet less as a single thing and more as an enormous, sprawling network of individually owned buildings. Each website is its own building, owned by its own company or person, with its own rules and its own level of trustworthiness. Your browser is the vehicle that carries you from building to building. Understanding that each site is a separate, independently run place, rather than one unified system, is the foundation for understanding why some sites are safe and others are not.

How Browsing Works

A browser is the app you use to visit websites. When you type an address or search for something, the browser fetches that page and displays it. The address bar at the top of the

screen is one of the most important safety tools you have: it tells you exactly where you actually are, which matters because scam websites are often built to look like real ones, sometimes down to the logo and color scheme.

Two small details in the address bar are worth learning to notice. First, the padlock icon, usually just to the left of the address, indicates the connection is encrypted, meaning information traveling between your device and that website is scrambled so it can't easily be intercepted. Second, the actual web address itself, often called a URL, is worth reading carefully rather than glancing past. A scam site might use an address like "amaz0n-support.com" instead of "amazon.com," hoping you won't look closely enough to notice the substituted zero.

TRY IT YOURSELF A Safe Browsing Scavenger Hunt

Open your browser and try each of these:

1. Look at the address bar. Do you see a small padlock icon? That means the connection is secure.
2. Search for "weather near me" and see what comes up.
3. Visit a website you trust, like your bank's

site, by typing the address yourself rather than clicking a link.

4. Notice the difference between a search result and an advertisement (ads are usually labeled “Ad” or “Sponsored”).

Search Engines and How They Choose Results

When you type a question into a search engine like Google or Bing, it is worth remembering that the top results are not always the most accurate or trustworthy; some are simply the ones that paid to appear there, or that are best at appearing relevant to a search engine’s software. This matters most when searching for something like a company’s phone number. Scammers have been known to purchase advertisements that display fake customer service numbers for well-known companies, so that a worried person searching for help ends up calling the scammer instead.

The safest approach, especially for anything involving your bank, a government agency, or a healthcare provider, is to go directly to the source. Use the address printed on a card in your wallet, on a past statement, or on the back of your insurance card, rather than

trusting a phone number you found through a search.

Email Basics

Email works like a digital version of postal mail; you have an address, and messages arrive in an inbox that only you can open, typically after entering a password. Unlike postal mail, however, anyone in the world with an internet connection can attempt to send you a message, which is part of why email is such a common scam tool. There is no postal worker checking identification before a message reaches your inbox.

Most email inboxes have some spam filtering built in, meaning suspicious messages are automatically sorted into a separate folder, usually labeled “Spam” or “Junk.” This filtering is helpful but imperfect. Some scam messages get through, and occasionally a legitimate message ends up incorrectly filtered out. It’s worth checking your spam folder occasionally, and worth treating anything in your main inbox with the same healthy skepticism regardless of which folder it landed in.

TRY IT YOURSELF Send a Practice Email

If you have a family member or friend who is willing, try this:

1. Open your email app.
2. Select “New Message” or the pencil/plus icon.
3. Type their email address in the “To” field.
4. Write a short message and a subject line.
5. Press send and ask them to reply so you can see a response arrive.

The Habits That Keep You Safe

A small number of habits prevent most everyday problems online. They are worth memorizing rather than just reading once, because they apply almost identically whether the threat arrives by email, text message, or phone call, and we will return to them throughout this book.

1. Pause before you click. Urgent language (“act now,” “your account will be closed”) is designed to make you skip this step. A legitimate company will almost never threaten to close your account within hours over an email.
2. Check who sent it. Tap or hover on a sender’s name to see the real email address,

not just the display name, which can be set to say anything the sender wants.

3. Go to the source directly. If you get a message claiming to be from your bank, don't click the link. Open your browser and type your bank's address yourself or call the number on your card.

4. When in doubt, ask. A trusted family member, friend, or your NAVIGATE facilitator would rather answer a question that turns out to be nothing than see you lose money to something that turned out to be real.

CHECKLIST Internet & Email Check

- ☐ I know how to tell if a website connection is secure (padlock icon).
- ☐ I know how to check who actually sent an email.
- ☐ I know not to click links in unexpected messages.
- ☐ I know how to type a website address directly instead of clicking a link.

Blocking Robocalls and Spam Texts

Unwanted robocalls, automated calls often used to deliver scam scripts at scale, remain one of the most common ways scam attempts reach older adults, alongside text messages

sent in bulk to enormous lists of phone numbers. Both your phone's carrier and your device itself offer tools to cut down on this traffic significantly and setting them up takes only a few minutes.

Most major carriers, including AT&T, Verizon, and T-Mobile, offer a free call-screening or spam-blocking service that can be turned on through your carrier's own app or by calling their customer service line directly. Your phone itself also has a built-in setting to silence calls from numbers not already in your contacts, sending them straight to voicemail instead of ringing through, which is a simple but effective way to ensure only calls from people you already know interrupt your day.

TRY IT YOURSELF Turn On Call Screening

On an iPhone: Settings, then Phone, then Silence Unknown Callers, and turn it on.

On an Android device: open the Phone app, tap the three-dot menu, then Settings, then Spam and Call Screen.

Ask your carrier (by phone or through their app) whether a free spam-blocking service is available and enabled on your line.

Subscription Traps and Free Trial Tricks

A subtler, less dramatic but still costly problem involves free trials that quietly convert into ongoing paid subscriptions. A product or service may advertise a free trial requiring only a credit card number to start, with the fine print noting that the card will be charged automatically once the trial period ends, unless canceled first. This is not, strictly speaking, illegal in most cases, but it is designed to rely on people forgetting to cancel, and it is worth building a habit around.

Whenever you sign up for any free trial, write down the exact date it converts to a paid subscription, either on a paper calendar or as a reminder in your phone, and set a reminder a few days before that date to decide, clearly, whether to keep it or cancel. Reviewing your bank and credit card statements regularly, a habit already recommended in Chapter 6, is also one of the best ways to catch a subscription you forgot about or never intended to keep paying for.

Many people notice, with some unease, that after searching for something like “walking

shoes,” advertisements for walking shoes seem to appear across nearly every website visited afterward. This happens through small pieces of tracking code called cookies, which websites use to remember your activity and share it with advertising networks. It is not a sign that your device has been compromised or that anyone is specifically watching you; it is standard, widespread advertising practice across the entire industry, and most browsers now offer settings to limit it if it feels intrusive, usually found under Settings, then Privacy.

Understanding this distinction matters because it helps separate ordinary, if unwelcome, advertising from genuine security threats. A pop-up ad for shoes is a nuisance. A pop-up claiming your device has a virus and demanding you call a phone number is a scam, covered in depth in Chapter 4. Learning to tell the two apart removes a significant amount of everyday anxiety.

Public Wi-Fi: What’s Actually Safe

Libraries, coffee shops, and senior centers often offer free public Wi-Fi, and it’s natural to wonder whether using it is safe. For ordinary browsing, checking the weather, reading news, or browsing recipes, public Wi-Fi is

generally fine. For anything involving sensitive information, logging into your bank, entering a password, or reviewing medical records, it is safer to wait until you're on a trusted home network, or to use your phone's own cellular data connection, which is considerably harder for someone nearby to intercept than an open public network.

Many public Wi-Fi networks require you to first open a browser and accept terms before connecting; this is normal. What is not normal is a Wi-Fi network prompting you to enter a password for an unrelated account, like your email or bank to "connect." No legitimate Wi-Fi network requires this, and any request like it should be treated as a red flag.

Understanding File Attachments

Email allows more than just text; it can carry attached files, documents, photos, or other content sent along with a message. Attachments are one of the more common ways malicious software spreads, because opening certain file types can install unwanted programs on your device without any additional warning. The safest general rule is to only open attachments from senders you recognize and were already expecting something from. An unexpected attachment,

especially one claiming to be an invoice, a shipping notice, or a document requiring your signature from a sender you don't recognize, is worth deleting rather than opening, even out of curiosity.

SPOT THE SCAM The Unexpected Invoice

An email arrives with the subject line "Invoice #4471 - Payment Overdue" from an unfamiliar company name, containing an attachment labeled "Invoice.pdf.zip" and a message reading: "Please review the attached invoice and remit payment within 24 hours to avoid late fees."

What's wrong here: you don't recognize the company, you weren't expecting an invoice, and the file ending in ".zip" after ".pdf" is a common trick to disguise a harmful file as an ordinary document. Delete the message without opening the attachment.

Choosing Safe Apps

Every app on your phone or tablet should come from one place: your device's official app store, meaning the App Store on Apple devices or Google Play on Android. Apps downloaded from a website, a text message link, or an email attachment bypass the review process these official stores perform

and are one of the more common ways harmful software reaches a device. If a website ever tells you to “download our app” through anything other than a link that opens the official App Store or Google Play, treat that as a warning sign rather than a convenience.

Even within an official store, it’s worth a quick check before installing anything new: look at how many people have downloaded the app and what recent reviews say, since a legitimate, well-established app typically has a long history and a large number of reviews, while a scam app mimicking a well-known brand often has very few downloads and reviews that mention problems. Before installing, the app will also show what permissions it requests, such as access to your camera, location, or contacts; if a simple game or calculator app asks for access that has nothing to do with its purpose, that mismatch is worth noticing and can be a reason to decline.

Recognizing Fake Online Reviews

Reviews are meant to help you judge a product, app or seller before committing to it, but a meaningful share of online reviews is fabricated, either by the seller themselves or

by paid review farms, especially for lesser-known products sold through large marketplaces. A cluster of five-star reviews all posted within the same few days, reviews that repeat the same unusual phrase, or a product with thousands of reviews but almost no photos from actual buyers are all worth treating with some skepticism.

It's often more useful to sort reviews by "most critical" or read the one- and two-star reviews first, since genuine complaints tend to describe specific, believable problems, while fake positive reviews tend to sound vague and enthusiastic without much real detail. This habit applies equally to app store reviews, online marketplace listings, and the hearing aid and other health product reviews covered in Chapter 7.

Organizing Your Digital Life

As you become more comfortable online, you'll likely accumulate a growing number of accounts, email, banking, healthcare portals, social media, each with its own username and password. Keeping a written record, stored somewhere physically secure like a locked drawer rather than a sticky note on your monitor, or using the password manager mentioned earlier in this chapter, prevents

the common and stressful problem of being locked out of an account you rarely use because the password has been forgotten.

It's also worth periodically reviewing which accounts you still use. Old accounts you've forgotten about, from a store you shopped at once or an app you tried years ago, still exist and still hold whatever information you originally provided. If one of those companies is ever affected by a data breach, an increasingly common event, an old, forgotten account can resurface as a security risk. Closing accounts, you no longer use is a small but genuinely protective habit.

MY NOTES

Chapter 4: Recognizing Scams & Fraud

Scams succeed for one main reason: they are built by people who study human psychology as carefully as any marketer, and they aim those tools at whatever will make you react before you think. This chapter is the longest single subject in this book for a reason. Everything else you learn about banking, healthcare, or government services online sits on top of the foundation built here.

It helps to start by removing any shame from the conversation. Fraud losses among older adults are not a reflection of intelligence or education. Studies from the FBI's Internet Crime Complaint Center and the Federal Trade Commission have repeatedly shown that people who lose money to scams span every education level and every walk of life, including retired professionals, former teachers, and people who spent entire careers managing other people's money. What separates people who avoid scams from people who don't is rarely intelligence. It is almost always a practiced habit of pausing.

The Architecture of a Scam

Nearly every scam, regardless of whether it arrives by phone, text, email, or a knock at the door, is built from the same three ingredients, combined in different proportions.

Urgency: you must act right now, or something terrible will happen. Your account will be frozen. Your grandchild will stay in jail another night. Your benefits will be cut off.

Authority: the message claims to come from someone you would normally trust and obey without question: a government agency, your bank, a police officer, or a family member.

Isolation: you're told, directly or indirectly, not to tell anyone else. "This is confidential." "Don't tell your family, it will only worry them." "If you tell anyone, the deal is off."

That last ingredient, isolation, is the one worth remembering most, because it is almost never present in a legitimate interaction. Real banks, real government agencies, and real family emergencies do not require secrecy from the rest of your support network. If a message or caller asks you to keep something from your family, that instruction alone is one of the strongest signals available that something is wrong.

Common Scam Categories

Scam tactics shift constantly in their specific packaging, but they tend to fall into a small number of recurring categories. Learning the category matters more than memorizing any single example, since a new variation of the same old category appears every few months.

The grandparent scam: a caller claims to be a grandchild in trouble, often citing an arrest, car accident, or hospital stay, and asks for money to be sent immediately, often through gift cards or wire transfer, and often begging you not to tell their parents.

The government impersonation scam: a caller claims to be from the IRS, Social Security Administration, or Medicare, warning of a legal problem, a suspended benefit, or a compromised account, and demanding payment or personal information to fix it.

The tech support scam: a pop-up window or phone call claims your computer has a virus, and a “technician” asks for remote access to your device or payment to fix a problem that does not actually exist.

The prize or sweepstakes scam: you’re told you’ve won a prize or lottery but must first pay a fee or taxes to claim it. Legitimate sweepstakes never require payment to release winnings.

The romance scam: covered in depth in Chapter 5, this involves a new online relationship that gradually moves toward requests for money, often tied to a supposed emergency or travel expense.

SPOT THE SCAM The Urgent Call

“This is Officer Daniels with the county sheriff’s department. Your grandson was in an accident and is being held pending bail. He asked us not to call his parents because he’s embarrassed. We need \$3,000 in gift cards sent today or he’ll be booked into county jail. Please don’t hang up.”

What’s wrong here: real law enforcement never requests bail or fines via gift cards, never asks you to keep an arrest secret from family, and never pressures for immediate payment over the phone. Hang up and call your grandson, or another family member, directly using a number you already have, not one given to you by the caller.

SPOT THE SCAM The Bank Text Message

“ALERT: Unusual activity detected on your account. Verify your identity immediately or your card will be suspended within 2 hours: [link]”

What's wrong here: legitimate banks rarely text urgent security alerts with a clickable link demanding immediate action, and they never ask you to "verify" your full account number, password, or Social Security number by text. Do not click the link. Open your banking app directly, or call the number printed on the back of your card.

SPOT THE SCAM The Delivery Text

"USPS: Your package could not be delivered due to an incomplete address. Update your delivery preferences here within 24 hours or the package will be returned to sender: [link]"

What's wrong here: postal and shipping carriers do not send text messages demanding you click a link to "update" an address, and this tactic works precisely because most people have a package in transit at any given time, making the message plausible regardless of who receives it. If you're genuinely expecting a delivery, check its status directly through the shipping carrier's official app or website, not through a link in an unexpected text.

SPOT THE SCAM The Job Offer That Pays

You First

A message arrives on a job site:

“Congratulations, you’ve been selected for our remote data-entry position, \$35/hour. To begin, we’ll mail you a check for equipment. Simply deposit it and wire back the difference to our equipment vendor.”

What’s wrong here: no legitimate employer sends money before you’ve done any work and asking you to deposit a check and wire part of it elsewhere is a classic sign the check itself is fraudulent and will eventually bounce, leaving you responsible for the full amount you already wired out. Legitimate remote job offers never involve depositing a check and forwarding money as a condition of employment.

The Psychology Behind Why It Works

It is worth understanding why urgency is such an effective tool, because the mechanism is biological, not a personal failing. When a person feels threatened or panicked, the brain shifts resources away from careful, deliberate thinking and toward fast, instinctive reaction. This is useful when facing a genuine physical danger. It is exactly what a scammer wants to trigger, because careful thinking is the enemy of every scam. The fix is not willpower in the

moment, since willpower is precisely what panic overrides. The fix is a rehearsed habit: hang up, log off, or close the message, and only decide what to do once you're calm.

TRY IT YOURSELF Build Your Pause Habit

Choose a single phrase you will say to yourself, out loud if it helps, the moment something feels urgent or frightening online or on the phone.

Some options:

"I don't make decisions under pressure."

"I'll call them back on a number I already trust."

"If it's real, it will still be real in an hour."

Write your chosen phrase here, and say it to someone in your NAVIGATE group so it feels real:

MY NOTES

Common Myths About Scams

A few widely held beliefs about scams turn out to be false and believing them can leave you less protected rather than more. It's worth correcting each one directly.

Myth: I'd definitely know if I were being scammed. Sophisticated scams are specifically designed not to feel like scams while they're happening. Confidence that you're immune is itself a vulnerability, since it can make you skip the verification habits in this chapter.

Myth: Scammers only target people who seem confused or isolated. Federal data shows victims span every education level and background, including people who spent entire careers in finance or law. Scammers target opportunity and momentary distraction, not a particular personality type.

Myth: If money left my account, it's gone, so there's no point reporting it. Some payment methods are recoverable, especially caught early, and even unrecoverable losses contribute to investigations that stop the same scammer from harming others. Reporting is never pointless.

Myth: Scammers are strangers from far away. As Chapter 6 covers, a substantial share of financial exploitation is carried out by

someone the victim already knows and trusts, not an anonymous stranger overseas.

Red Flags Worth Memorizing

While tactics vary, certain warning signs appear across nearly every scam category. Committing this list to memory is one of the single highest-value things you can do for your own safety.

CHECKLIST Scam Red Flags

- ☐ Contact was unexpected: I didn't initiate this call, text, or email.
- ☐ There's pressure to act immediately, without time to think.
- ☐ I'm being asked to pay with gift cards, wire transfer, or cryptocurrency.
- ☐ I'm told to keep this secret from family or friends.
- ☐ I'm asked for personal information I wouldn't normally give out.
- ☐ Something about the request doesn't match how this organization normally contacts me.

If even one of these applies, that is reason enough to pause, hang up, and verify independently before doing anything else. You will never be penalized by a legitimate organization for taking time to verify. That

single fact, that real institutions do not punish caution, is worth holding onto.

A Closer Look: The Investment and Cryptocurrency Scam

A newer, and often more financially devastating, category of scam involves fraudulent investment opportunities, frequently tied to cryptocurrency. These scams often begin innocuously, sometimes through a social media ad promising an experienced trader will teach you how to grow your savings, or through an initial small, genuine payout designed to build confidence before larger amounts are requested. Victims are often directed to a professional-looking website or app displaying a growing account balance that is entirely fabricated, showing numbers the scammer controls rather than money that exists anywhere.

The warning signs here overlap heavily with the general patterns already covered: promises of unusually high, guaranteed returns; pressure to invest quickly before a supposed opportunity closes; and, most tellingly, difficulty ever actually withdrawing money once it has been deposited, often met with new fees or taxes that must supposedly be paid first. Legitimate investments never

guarantee specific returns, and legitimate financial advisors are licensed and can be verified through your state's securities regulator.

SPOT THE SCAM The Trading Group

A former coworker adds you to a group chat where members share screenshots of huge trading profits, and a friendly “mentor” offers to personally manage a small initial investment for you, promising to double it within a month. After sending \$500, your account balance in the app does indeed appear to double. The mentor now suggests you’re ready to invest \$10,000 for a much larger return.

What’s wrong here: guaranteed, unusually high returns and pressure to escalate your investment quickly are hallmark signs of a pyramid-style investment scam, sometimes called a Ponzi scheme. The early “profit” is often bait, either a real but small payout funded by other victims’ deposits, or simply a number displayed on a screen with no real money behind it. Before investing any significant amount with anyone, verify their license through the Financial Industry Regulatory Authority’s free BrokerCheck tool, available at brokercheck.finra.org.

A Closer Look: The Overpayment Scam

This scam typically targets people selling something online, whether through a classified ad, a garage sale posting, or a marketplace app. A buyer sends a check or electronic payment for more than the agreed price, then asks you to refund the difference, often citing a shipping company error or a family member who supposedly overpaid on their behalf. The original payment, however, is fraudulent and will eventually bounce or be reversed by the bank, days or weeks later, after you've already sent your own genuine money back as a "refund."

The core lesson generalizes well beyond this specific scenario: funds shown as available in an account, whether a check that has been deposited or a payment app balance, are not the same as funds that have been fully and irreversibly cleared, which can take significantly longer than the amount showing as available might suggest. Never send money back in response to an overpayment; instead, ask the buyer to cancel and resend the correct amount.

The Sandwich Generation and Shared Vigilance

Many readers of this book are not only managing their own digital safety but also

helping aging parents or supporting adult children who are themselves managing young families, sometimes all at once. If you find yourself in this position, it's worth extending the habits in this chapter outward: talk openly with parents, siblings, and adult children about scam tactics, since a family that discusses this topic openly, without embarrassment, catches far more attempted fraud than one where the subject feels taboo.

Consider setting a standing, informal rule within your own family: any request for money, no matter who it appears to come from or how urgent it seems, gets a phone call to a second family member before any action is taken. This single habit, sometimes called the two-person rule in fraud prevention circles, catches a remarkable share of otherwise convincing scams, simply by introducing a brief pause and a second, less emotionally invested set of eyes.

What the Numbers Say About Each Scam Type

Federal crime data helps put each scam category in perspective. In 2025, the FBI's Internet Crime Complaint Center recorded investment fraud, much of it now tied to cryptocurrency, as the single largest loss

category among older victims, totaling several billion dollars, followed by tech support scams and romance scams. Government and business impersonation scams, the categories covered earlier in this chapter, remain both the most common in terms of sheer number of reports and consistently among the most damaging per incident.

One more figure is worth knowing, because it reframes what “vulnerability” means: the FTC has found that older adults are, in fact, somewhat less likely than younger adults to lose money once a scam attempt reaches them, which researchers believe reflects greater caution and life experience, not less. The real danger is not lower resistance. It is that when an older adult’s caution is successfully overcome, often through a highly sophisticated, well-funded operation, the resulting loss tends to be considerably larger, since scammers investing significant effort in a single target tend to pursue a bigger payout.

Grief and Holiday Scams

Scammers deliberately time certain tactics to moments of heightened emotion or distraction. In the days after a loved one’s passing, scammers sometimes monitor

published obituaries for names and details, then call surviving family members posing as a collections agency claiming the deceased had an outstanding debt that must be settled immediately, a debt that in reality does not exist, since a deceased person's individual debts are not legally transferable to family members in the way these callers claim.

Similarly, the holiday season and major shopping events see a sharp seasonal rise in fake shipping notifications, charity impersonation scams, and too-good-to-be-true online deals. The same core habits from earlier in this chapter, verifying independently and never acting under pressure, apply here without modification; scammers change their seasonal costume, but not their underlying method.

Charity Scams After a Disaster

Within hours of a major hurricane, wildfire, or earthquake making the news, fraudulent fundraising pages and lookalike charity websites reliably appear, built to capture some of the genuine wave of generosity a disaster produces. These fake operations often use professional-looking logos, stolen photos from real news coverage, and emotionally charged language, and can be

difficult to distinguish from a legitimate relief effort at a glance.

A few checks protect your donation. Give to established charities with a track record you already recognize, rather than one that seems to have appeared overnight tied to the current headline. Before donating to an unfamiliar organization, check it against a charity watchdog site such as Charity Navigator or the BBB's Give.org, both free to use. Pay by credit card, which preserves your right to dispute the charge, rather than by gift card, wire transfer, or cryptocurrency, all frequently requested by fraudulent charities specifically because they're difficult to trace or reverse.

SPOT THE SCAM The Disaster Relief Text

The morning after a hurricane makes national news: "Urgent: Hurricane victims need YOUR help NOW. Text DONATE to give \$50 instantly to families who lost everything. 100% goes directly to victims."

What's wrong here: legitimate charities rarely claim 100 percent of a donation bypasses all overhead, since even efficient organizations have some operating costs, and an organization with no prior name recognition appearing within

hours of a disaster is a pattern regulators specifically warn about. Look up an established, recognized relief organization directly rather than donating through an unfamiliar text link.

CHECKLIST Family Vigilance Plan

- ☐ My family has discussed common scam tactics openly, at least once.
- ☐ We have a two-person rule: no money moves without a second family member's input.
- ☐ Everyone in my immediate family knows our safe word (see Chapter 5).
- ☐ I know who in my family I'd call first if something felt wrong.

TALK ABOUT IT

Has anyone in your family or circle of friends ever described a scam attempt to you? What made them suspicious, or what almost convinced them?

MY NOTES

Chapter 5: AI, Deepfakes & Romance Scams

Of everything covered in this book, the material in this chapter has changed the fastest, and will likely keep changing. Artificial intelligence tools now allow scammers to fabricate convincing voices, photographs, and even video of real people, at a level of realism that would have been the domain of Hollywood studios only a few years ago. This chapter will not try to catalog every current tool, since that list will be outdated quickly. Instead, it focuses on the underlying pattern, which changes far more slowly than the technology itself.

What a Deepfake Actually Is

A deepfake is a piece of audio, a photograph, or a video that has been artificially generated or altered by a computer program to make it appear that a real person said or did something they never actually said or did. The technology works by studying many real recordings or photographs of a person and using that pattern to generate new, fabricated material that mimics their voice or appearance.

The unsettling part is how little original material a program now needs. A scammer may only need a few seconds of a person's voice, sometimes pulled from a public social media video or voicemail greeting, to generate a convincing fake recording. This is part of why Chapter 10's guidance on social media privacy matters directly here: the less public audio and video of your voice and face that exists online, the less raw material a scammer must work with.

The Voice Cloning Scam

A newer variation on the classic grandparent scam uses a cloned voice instead of, or alongside, a scripted actor. A caller plays a short, distressed audio clip that sounds exactly like your grandchild, saying something like "Grandma, it's me, I'm in trouble," before a second voice, posing as an authority figure, takes over the call to demand payment. Because the voice sounds genuinely familiar, the emotional impact is far stronger than a scam call from a stranger.

SPOT THE SCAM The Cloned Voice

A shaky, tearful voice that sounds exactly like your granddaughter says: "Grandma, please, I got in a car accident and I'm at the police

station, please don't tell mom, this man is going to explain what to do." A calm male voice then takes over the call.

What's wrong here: the emotional intensity and request for secrecy are the same red flags from Chapter 4, regardless of how convincing the voice sounds. Hang up immediately and call your granddaughter directly on a number you already have saved. If she doesn't answer, call her parents or another family member. A cloned voice cannot answer a phone that is in her pocket.

The single most reliable defense against a voice cloning scam is one your family can set up together in advance: a family safe word. Agree on a simple word or phrase, unrelated to anything discoverable online, that any real family member would know and use if they ever called in a genuine emergency asking for money. If a caller claiming to be a relative cannot provide it, treat the call as fraudulent and hang up.

TRY IT YOURSELF Set Up a Family Safe Word

Talk with your immediate family and agree on a word or short phrase nobody outside the family

would guess.

Write it down somewhere private, not in a place a scammer could plausibly find it, such as posted publicly on social media.

Agree together: if anyone calls claiming to be in trouble and asking for money, the safe word is required before any money moves.

Recognizing AI-Generated Images and Video

AI-generated images have distinctive, though shrinking, flaws. Hands with too many or too few fingers, unnatural skin texture, blurred or inconsistent backgrounds, and eyes that don't quite focus the same direction have all been common tells. These flaws are becoming rarer as the technology improves, which means visual inspection alone is becoming a less reliable defense than it was even a year or two ago. The more durable defense is the same one that runs through this entire chapter: treat any unexpected request involving money or personal information with the same skepticism regardless of how convincing the supporting evidence looks or sounds.

Live, real-time video deepfakes, where a scammer appears to impersonate someone's face and voice during an actual video call

rather than a pre-recorded clip, remain considerably harder to produce convincingly than a still image or short recording, since they require processing a live feed instantly. This is part of why the video-call verification approach recommended throughout this chapter remains one of the strongest tools available today. That said, this is precisely the kind of gap most likely to close as the technology improves further, so treat video confirmation as a strong current safeguard rather than a permanent guarantee and keep pairing it with the family safe word covered earlier in this chapter.

Romance Scams

Romance scams typically begin on a dating site, a social media platform, or occasionally through an unexpected friendly message from a stranger. The scammer, often operating from overseas as part of an organized operation, invests real time, sometimes weeks or months, in building what feels like a genuine emotional connection before ever mentioning money.

The eventual request for money is rarely presented as a simple ask. It typically arrives wrapped in a plausible emergency: a medical bill, a stuck shipment of valuable goods held

at customs, a business opportunity you're invited to join, or travel costs to finally meet in person. Because real trust and affection have been built first, the emotional pull to help is genuine and strong, which is precisely why romance scams are so financially devastating and so difficult for the person experiencing one to recognize from the inside.

SPOT THE SCAM The Long-Distance Romance

After three months of daily messages with someone you met on a social app, who says they're a widowed engineer working on an offshore oil rig, they write: "My darling, I finally have enough saved to come see you, but customs is holding my equipment and I need \$4,000 to release it. I will pay you back the moment I arrive, I promise."

What's wrong here: a request for money before ever meeting in person, an inability or unwillingness to video call, and a story involving customs, shipping, or a remote work location are all extremely common romance scam patterns. Legitimate romantic interest does not require you to wire money to someone you have never met face to face.

CHECKLIST Romance Scam Warning Signs

- ☐ We have never met in person, and video calls are always postponed or avoided.
- ☐ Their profile photos look professionally taken, or oddly perfect.
- ☐ The relationship moved to declarations of love very quickly.
- ☐ They have a story involving overseas work, military deployment, or international shipping.
- ☐ Money has come up, in any amount, for any reason.

If two or more of these apply, it is worth having an honest conversation with someone you trust about the relationship, even if it feels difficult. This is not a judgment about your ability to love or connect with another person. It is a recognition that a determined, organized scammer is specifically trained to be convincing, and a second, less emotionally invested perspective is one of the most effective tools available for seeing clearly.

How AI Tools Are Changing Everyday Scams

Beyond voice cloning and romance scams, artificial intelligence has begun quietly reshaping nearly every scam category covered in Chapter 4. Text-based scam messages, once often identifiable by awkward grammar or obvious spelling mistakes, a telltale sign scammer themselves have relied on for years, are now frequently written by AI language tools capable of producing fluent, natural-sounding English indistinguishable from a genuine message. This means the old advice of “watch for bad grammar” is becoming steadily less reliable as a warning sign, and the structural red flags covered in Chapter 4, urgency, authority, and isolation, matter more than ever precisely because surface-level polish can no longer be trusted to reveal a fake.

AI tools have also made it dramatically easier for scammers to generate large volumes of highly personalized messages at once. A scammer might scrape publicly available information about you, your workplace history, your hometown, your children’s names, from social media or public records, and feed it into an AI tool that generates a message referencing those specific details, making an otherwise generic scam feel eerily personal and credible. This is, again, a strong

argument for the privacy habits covered in Chapter 10: the less specific personal information sits publicly online, the less raw material exists for this kind of targeted, AI-assisted attack.

Fake Websites and Storefronts

AI image and web design tools have also made it far easier to build entire fake online storefronts quickly and cheaply, complete with professional-looking product photos, that never deliver purchased items or deliver something far different and cheaper than advertised. These fake stores frequently appear through social media advertisements offering steep discounts on popular brand-name products.

A few checks help before buying from an unfamiliar online store: search the store's name along with the word "reviews" or "scam" before purchasing; be suspicious of prices dramatically below a product's normal retail price; and always use a credit card rather than a debit card or direct bank transfer for online purchases from unfamiliar sellers, since credit cards offer stronger fraud protection and dispute rights under federal law.

TRY IT YOURSELF Research Before You Buy

Before purchasing from an unfamiliar online store, take two minutes to:

1. Search the store's name plus the word "reviews."
2. Check whether the store has a real, physical customer service address listed.
3. Confirm you're paying with a credit card, not a bank transfer or gift card.

Fake Customer Service and AI Chatbots

A newer tactic involves scammers building fake customer service chat windows, sometimes appearing on a fraudulent website and sometimes inserted into search results as a paid advertisement, that mimic a real company's support chat closely enough to fool a careful shopper. Some of these are staffed by real people; increasingly, some are automated using AI chatbot tools, capable of holding a convincing, natural conversation while steering it toward requesting payment information or remote access to your device.

The safest habit here is the same one from Chapter 3: reach customer support only through a link or number found on the company's official website, typed in yourself,

never through a chat window that appeared unprompted, a pop-up, or a number found through a general search. If a “support agent,” human or automated, ever asks you to install remote-access software so they can “fix” something on your device, that request itself is one of the strongest scam signals covered anywhere in this book, regardless of how legitimate the rest of the conversation seemed.

SPOT THE SCAM The Fake Support Chat

While searching for your bank’s customer service number, a chat window pops up: “Hi, I’m Sam from support. I can see there’s an issue with your account. Let’s get this resolved right now, can you download our secure access tool so I can take a look?”

What’s wrong here: this chat appeared unprompted rather than through a link you navigated to on the bank’s actual website, and no legitimate support chat asks you to install remote-access software within the first message. Close the window and navigate to your bank’s site or app directly.

Staying Grounded as Technology Changes

It would be reasonable, after reading this chapter, to feel that keeping up with AI-driven scams is an impossible, moving target, since the specific tools will undoubtedly keep changing after this book is printed. That feeling is understandable, but it misses the more durable truth underlying this entire book: the emotional tactics scammers rely on, urgency, authority, and isolation, have remained essentially unchanged for decades, long before any of these technologies existed. AI has changed the packaging. It has not changed the underlying con.

This is why the pause habit from Chapter 4 remains your single most reliable defense, regardless of how convincing a voice, a photo, or a message becomes. A rehearsed habit of slowing down and verifying independently works exactly as well against a scam that didn't exist, yet when this book was written as it does against one described in these pages.

A Conversation Worth Having with Family

Given how central family trust is to many of the scams described in this chapter, it's worth having an explicit conversation, not just an implied understanding, with the people closest to you about how you'll handle a

genuine emergency request for money in the future. Beyond the safe word exercise earlier in this chapter, agree together on a specific process: who gets called first, what verification steps will always happen before money moves, and an explicit agreement that no family member will ever be upset with another for taking time to verify, even if a request turns out to be genuine.

TALK ABOUT IT

Bring up this chapter with your family directly. Ask: if I called you sounding panicked and asking for money, what would you want me to do to make sure it was really you?

MY NOTES

Chapter 6: Banking & Financial Safety Online

Online banking, when set up carefully, is genuinely safer than many of the alternatives it replaced. A stolen paper checkbook or a mailed bank statement pulled from an unlocked mailbox has historically been a common source of fraud. Digital banking, protected by the right settings, closes many of those older vulnerabilities while opening a few new ones this chapter will help you close as well.

Getting Comfortable with Your Bank's App or Website

Most banks now offer both a website and a dedicated app. Either is safe to use, provided you access it correctly: type your bank's address directly into your browser, or download the app only from your device's official app store (the App Store on Apple devices, or Google Play on Android), never from a link in a text message or email.

Once logged in, take time to simply look around before doing anything else. Notice where your account balance is displayed, where recent transactions are listed, and

where you would go to send money or pay a bill. Familiarity with the ordinary layout of your own banking app is itself a security tool, since it makes an unfamiliar, fraudulent-looking screen much easier to notice.

TRY IT YOURSELF Explore Your Banking App Safely

Open your bank's official app or website (not from an email link).

Find your account balance and note where it's displayed.

Find your recent transaction history.

Find the customer service phone number listed inside the app or site and compare it to the number on the back of your card.

Passwords That Actually Protect You

A strong password is longer than most people expect it needs to be. Security researchers now generally recommend passwords of at least twelve characters, and increasingly suggest thinking in terms of a passphrase, several unrelated words strung together, rather than a single word with a number and symbol added on. "Correct Horse Battery Staple" style passphrases are both easier to remember and harder for a computer program to guess than something like

“Fluffy1!”, because length matters more to a computer guessing passwords than complexity does.

Reusing the same password across multiple accounts is one of the most common and most damaging habits in digital security. If one company’s records are ever exposed, and unfortunately this happens to well-known companies often, criminals will try that same password against your email, your bank, and every other account they can find. A password manager, mentioned in Chapter 2, solves this problem by generating and remembering a unique password for every single account, so you only need to remember one master password yourself.

Two-Factor Authentication, Explained Simply

Two-factor authentication, often abbreviated 2FA, adds a second lock to your accounts beyond just a password. After entering your password, the account sends a temporary code to your phone by text message or requires you to approve the login from another device you already trust. Even if a criminal somehow learns your password, they still cannot get into your account without also having physical access to your phone.

This single feature is one of the most effective, and most underused, protections available to you. Banks, email providers, and most major websites now offer it, usually found under a section of settings called “Security” or “Login & Security.”

TRY IT YOURSELF Turn On Two-Factor Authentication

Open your bank’s app or website and look for Settings, then Security.

Look for an option called “Two-Factor Authentication,” “2FA,” or “Login Verification.”

Follow the prompts, usually confirming your phone number to receive text codes.

Repeat this same search for your primary email account. Protecting your email matters as much as protecting your bank, since email is often used to reset other passwords.

Recognizing Financial Fraud in Progress

Beyond the scam patterns already covered in Chapter 4, a few warning signs are specific to banking and financial accounts. A legitimate bank will never call, text, or email asking you to read back a two-factor authentication code you just received; if someone asks for that code, they are trying to log into your account

themselves while you unknowingly provide the key. A legitimate bank will also never ask you to move money into a “safe” or “protected” account they specify, a tactic sometimes used in elaborate scams involving fake fraud alerts.

SPOT THE SCAM The Fake Fraud Alert

You receive a call: “This is the fraud department. We’ve detected an unauthorized \$2,000 charge. To reverse it and protect your remaining funds, we need to move your money to a temporary secure account. Can you confirm the verification code we just texted you?”

What’s wrong here: real fraud departments do not ask you to move your own money to a different account and never ask you to read back a verification code, since that code exists specifically to prevent someone else from accessing your account. Hang up and call the number on the back of your card directly.

Your Rights as a Banking Customer

Federal law provides several protections worth knowing by name, since they set a floor beneath what any bank or card issuer is legally required to do for you. The Electronic Fund Transfer Act limits your liability for

unauthorized electronic transfers, provided you report them promptly, generally within 60 days of your statement. The Fair Credit Billing Act gives you the right to dispute credit card charges in writing and requires the card issuer to investigate. And the Truth in Lending Act requires clear disclosure of loan and credit terms, including interest rates and fees, before you agree to them.

None of these require memorizing legal text. The practical takeaway is simpler: you have real, enforceable rights when something goes wrong with a bank or credit account, this book's advice to report issues quickly isn't just good practice, it's what activates the legal protections you're already entitled to, and a bank that resists a legitimate dispute can be reported to the Consumer Financial Protection Bureau, which exists specifically to enforce these protections.

Checking Your Accounts Regularly

One of the simplest habits in this entire book is also one of the most protective: checking your account activity regularly, ideally weekly, rather than waiting for a monthly paper statement. Catching a fraudulent charge within days rather than weeks dramatically improves your chances of

recovering the money and limiting further damage. Many banking apps also allow you to set up automatic alerts for any charge over an amount you choose, which does this watching for you.

Understanding How Money Actually Moves

It helps to understand in plain terms what happens when you move money electronically, since this knowledge directly explains several of the safety rules in this chapter. A wire transfer moves money almost instantly and, critically, is very difficult or impossible to reverse once sent, which is exactly why scammers favor it. A standard bank transfer or bill payment through your bank's own app typically takes one to three business days and offers more opportunity to catch and stop a mistake. Payment apps like Zelle, Venmo, and Cash App sit somewhere in between: they move quickly, often instantly, and are generally intended for sending money to people you already know personally, like splitting a dinner bill, not for paying strangers or unfamiliar sellers, since they offer very limited fraud protection compared to a credit card.

This distinction is worth committing to memory: credit cards offer the strongest legal protection if something goes wrong, since federal law limits your liability for unauthorized charges and gives you a formal right to dispute a charge. Debit cards offer weaker protection, since the money leaves your account immediately. Wire transfers, gift cards, and cryptocurrency offer essentially no protection at all once sent. When you have a choice in how to pay, this hierarchy is worth keeping in mind.

How to Dispute a Charge

If you spot a charge on your credit or debit card statement that you don't recognize or didn't authorize, federal law gives you the right to dispute it, and the process is more straightforward than many people expect. Start with your card issuer directly, either through their app, website, or by calling the number on the back of your card and report the charge as unauthorized or incorrect. The issuer is generally required to investigate and respond within a set timeframe, and in most cases will issue a temporary credit to your account while the investigation is ongoing, so you aren't out the money while it's being resolved.

Keep a simple record as you go: the date you reported the charge, who you spoke with, and any confirmation or case number provided. If a dispute is denied and you believe that's incorrect, you have the right to ask for a written explanation and to escalate the complaint, including to the Consumer Financial Protection Bureau, which accepts complaints about financial companies at no cost.

Verifying a Financial Advisor

If someone approaches you, or you're referred to someone, offering to manage your investments or retirement savings, it's worth verifying their credentials before handing over any money, regardless of how the introduction came about. Legitimate investment professionals are required to be registered, and you can check any advisor's registration, disciplinary history, and background entirely for free through the Financial Industry Regulatory Authority's BrokerCheck tool at brokercheck.finra.org, or the SEC's Investment Adviser Public Disclosure database.

A genuine advisor will never object to you taking time to verify their credentials, and will never guarantee a specific investment return,

since all legitimate investments carry some risk. Pressure to invest quickly, secrecy about fees, or reluctance to put recommendations in writing are all reasons to slow down and verify independently before moving any money, echoing the same pause-and-verify habit from Chapter 4.

Credit Freezes and Fraud Alerts

Beyond the reactive step of freezing your credit after a scam, covered in Chapter 12, you can proactively place a credit freeze at any time, even without a specific incident prompting it. A freeze prevents new credit accounts from being opened in your name at all, since lenders cannot check your credit report while it's frozen, which stops most forms of new-account identity theft in its tracks. It is free, and it can be temporarily lifted whenever you genuinely need to apply for credit yourself, then reinstated afterward.

A fraud alert is a lighter-touch alternative, requiring lenders to take extra verification steps before opening new credit in your name, without fully blocking access the way a freeze does. Many financial counselors recommend a full freeze for anyone not actively planning to apply for new credit or loans, simply because

it offers the strongest protection with almost no downside for most retirees.

Financial Exploitation by Someone You Know

This book has focused mainly on strangers and organized scam operations, but it's important to name a harder truth directly: research from the Consumer Financial Protection Bureau and similar bodies has found that a large majority of elder financial exploitation, by some estimates around 72 percent, is carried out not by a stranger but by someone the older adult already knows and trusts, including family members, caregivers, or new acquaintances who work their way into a position of influence. The Department of Justice's own reporting has found more than 2 billion dollars taken from older Americans through this kind of exploitation in a single recent reporting period, separate from the stranger-scam figures cited earlier in this book.

This category of harm is often described as "hidden" because it rarely looks dramatic from the outside. It tends to begin quietly: a family member offering to help manage bills who gradually starts moving money for themselves; a new friend or companion who

becomes unusually involved in financial decisions; a caregiver who begins pressuring for gifts, loans, or changes to a will or power of attorney. Financial counselors and elder law attorneys point to a consistent set of warning signs worth knowing, regardless of who is involved.

CHECKLIST Signs Worth Paying Attention To

- ☐ Unexplained withdrawals, transfers, or new authorized users on an account.
- ☐ Bank or credit card statements that stop arriving, or that someone else insists on handling.
- ☐ Sudden, unexplained changes to a will, deed, or power of attorney.
- ☐ A new person in your life who becomes unusually involved in financial decisions quickly.
- ☐ Feeling pressured, fearful, or reluctant to discuss finances around a specific person.

If any of this feels familiar, either about your own situation or someone you care about, it's worth knowing that every state has an Adult Protective Services agency, reachable through the Eldercare Locator number in Chapter 13, specifically tasked with

investigating exactly this kind of concern, confidentially and without requiring certainty before reaching out. Raising a concern, even a tentative one, is not an accusation; it is a request for a trained professional to investigate a situation you're not equipped to fully assess alone. An estate planning or elder law attorney, also mentioned in Chapter 9, can separately help review or adjust legal protections like a power of attorney if that becomes necessary.

CHECKLIST Banking Safety Check

- ☐ I access my bank only through the official app or a website I typed myself.
- ☐ I have a unique password for my banking account, not reused elsewhere.
- ☐ Two-factor authentication is turned on for my bank and my email.
- ☐ I check my account activity at least weekly.
- ☐ I know the real customer service number for my bank, saved somewhere I can find it.

TALK ABOUT IT

Ask a family member to help you set up account alerts for unusual charges this week and pick a day to check together that it worked.

MY NOTES

Chapter 7: Healthcare Systems Online

Healthcare has moved online faster than almost any other part of daily life over the past decade. Patient portals now hold lab results, appointment scheduling, prescription refills, and direct messages with your care team. Telehealth visits, conducted by video call, have become a routine option rather than an emergency workaround. This chapter walks through both, along with how to keep your health information as protected as your financial information.

Understanding Patient Portals

A patient portal is a secure website or app, provided by your doctor's office, hospital system, or insurance company, where you can view your own medical records. Common platforms include MyChart, used by many hospital systems, and portals specific to individual insurance companies like Medicare's own online account system.

Setting one up typically requires an invitation from your provider's office, often sent by email or given to you on a printed sheet after a visit, containing a special activation code. If

you haven't set up a portal account yet, it is worth asking your doctor's office directly at your next visit rather than searching for it online, since this avoids any risk of landing on an imitation site.

TRY IT YOURSELF Explore a Patient Portal

If you already have a patient portal account, log in and look for:

1. Your most recent lab results or visit summary.
2. The messaging feature to contact your care team directly.
3. The appointment scheduling section.

If you don't yet have an account, write down the name of your primary doctor's office so you can ask about portal access at your next visit or call.

Telehealth Visits

A telehealth, or telemedicine, appointment is a medical visit conducted over video call rather than in person. It typically works through a link sent by your provider's office, either by text or email, which opens directly into a video call at your scheduled time, usually without needing to download a separate app.

Telehealth is particularly useful for follow-up appointments, medication check-ins, and mental health visits, where a physical examination isn't required. It is worth asking your provider directly which types of visits they offer this way, since availability varies by practice.

TRY IT YOURSELF Prepare for a Telehealth Visit

Find a quiet, well-lit spot in your home, ideally near your Wi-Fi router for a strong connection.

Test your device's camera and microphone a day before the appointment, if possible, not right at appointment time.

Have a list of your current medications and questions written down beforehand, just as you would for an in-person visit.

Only click a telehealth link sent directly by your provider's office; never one sent by an unexpected text claiming to be a doctor you don't recognize.

Protecting Your Health Information

Health information is valuable to criminals for a different reason than banking information: it can be used to file fraudulent insurance claims, obtain prescription drugs, or even receive medical treatment under your

identity, a problem that can take far longer to untangle than a stolen credit card number. Federal privacy law, specifically HIPAA, requires healthcare providers to protect your information carefully, but scammers often try to bypass this protection by impersonating a provider directly rather than attacking the provider's systems.

SPOT THE SCAM The Fake Medicare Call

"This is calling from Medicare regarding your new benefits card. We just need to verify your Medicare number and Social Security number to process your upgraded coverage."

What's wrong here: Medicare already has your Medicare number on file and will never call asking you to "verify" it or your Social Security number over the phone. Hang up and, if concerned, call Medicare directly using the number on the back of your Medicare card or on a statement you already have.

Reviewing Your Explanation of Benefits

After most medical visits, your insurance company or Medicare sends a document

called an Explanation of Benefits, often abbreviated EOB, listing the services billed. Reviewing this document, even briefly, is one of the most effective ways to catch medical identity fraud early, since it will show any service billed under your name that you don't recognize. Many insurers now make this document available directly in their online portal, often faster than the mailed paper version arrives.

Understanding Your Rights Under HIPAA

The Health Insurance Portability and Accountability Act, commonly known as HIPAA, gives you specific legal rights over your own medical records that are worth knowing. You have the right to request and receive a copy of your medical records from any provider, generally within 30 days of asking. You have the right to know who your information has been shared with. And you have the right to request corrections if you find an error in your record. Understanding these rights matters because scammers sometimes rely on people not knowing what a legitimate records request or disclosure looks like, making it easier to impersonate one.

It's worth noting what HIPAA does not do: it does not prevent you from sharing your own

medical information with family members if you choose to, and it does not prevent your own doctor's office from calling you directly about your own care. The rule protects your information from being shared by others without your permission; it does not restrict your own ability to manage and discuss your own health.

Choosing a Care Proxy or Medical Power of Attorney

Many older adults choose to designate a trusted family member or friend as a healthcare proxy, sometimes called a medical power of attorney, someone legally authorized to make medical decisions on your behalf if you're ever unable to make them yourself. Most patient portals allow you to formally link a proxy's account to your own, so they can view records and communicate with your care team directly when needed, rather than relying on you to relay information during a stressful moment.

Setting this up in advance, while you're feeling well and can think it through calmly, is far easier than trying to arrange it during a medical crisis. It is worth raising with your doctor's office directly, since the specific

paperwork required varies somewhat by state and by healthcare system.

Shopping for Hearing Aids Without Getting Scammed

Since 2022, federal rules have allowed hearing aids for adults with mild to moderate hearing loss to be sold over the counter, without a prescription or hearing exam, which has genuinely lowered costs and expanded access for millions of people. That same openness, unfortunately, has also drawn scammers into the market, selling cheap, poorly performing devices, or products that aren't hearing aids at all, dressed up with misleading marketing aimed specifically at older adults.

A few warning signs are worth knowing before buying. Legitimate over-the-counter hearing aids are required to be clearly labeled as “OTC hearing aid”; a product labeled only as a “personal sound amplifier” is a different category of device not designed to treat hearing loss, whatever the marketing implies. Be skeptical of listings, especially on general marketplaces, that stuff their titles with every possible search term at once, of claims to be “FDA-approved” (the FDA does not approve individual hearing aid brands this way), and of

prices dramatically below typical market rates. A reputable seller offers a real trial period, typically at least 30 days, and has easy-to-find customer support, not just a social media page.

As with any online purchase covered elsewhere in this book, paying by credit card rather than other methods preserves your ability to dispute the charge if the product turns out to be misrepresented, and if you do encounter a scam, the FTC's reportfraud.ftc.gov, listed in Chapter 13, is the right place to report it.

Mental Health Support Through Telehealth

Telehealth has made mental health counseling considerably more accessible for many older adults, particularly for those managing mobility limitations, transportation barriers, or simply a preference for privacy that an office visit doesn't offer. Medicare covers telehealth mental health visits, including counseling and psychiatric care, generally at the same rate as an in-person visit, and many private Medicare Advantage and supplemental plans follow suit.

If you're considering counseling but unsure where to start, your primary doctor's office can typically provide a referral, and many patient portals, covered earlier in this chapter, now let you search for and book a mental health visit the same way you'd book any other appointment. Grief, isolation, and the anxiety that can come with navigating unfamiliar technology or a recent scam experience, covered in Chapter 12, are all common, legitimate reasons to seek this kind of support, not signs of weakness.

CHECKLIST Healthcare Safety Check

- ☐ I have set up, or plan to ask about, a patient portal account with my primary doctor.
- ☐ I know how to join a telehealth video visit when scheduled.
- ☐ I know Medicare and my insurer will never call asking me to verify my number.
- ☐ I review my Explanation of Benefits statements for services I don't recognize.

TALK ABOUT IT

Ask your doctor's office at your next visit which of their services are available through the patient portal or by telehealth.

MY NOTES

Chapter 8: Government Services Online

Social Security, Medicare, the IRS, and your state's own agencies increasingly conduct business online, from checking your benefit statements to filing taxes to renewing a driver's license. This shift can genuinely save time and hassle, but government impersonation remains one of the single most common scam categories aimed at older adults, which makes this chapter especially important to read carefully.

The Golden Rule of Government Contact

It is worth stating this plainly, because it resolves most of the confusion in this area: government agencies overwhelmingly initiate contact with you by official mail, not by phone call, text message, or email. The Social Security Administration, the IRS, and Medicare will not call you out of the blue demanding immediate payment, threatening arrest, or asking you to verify your Social Security number to “reactivate” a benefit. If you receive a call like this, the safest response is always the same: hang up, and if you're concerned there may be a genuine issue, contact the agency directly using a number

you look up independently, not one given to you by the caller.

SPOT THE SCAM The Jury Duty Call

“This is Deputy Marshal Collins. Court records show you failed to appear for jury duty last week, and a warrant has been issued. You can resolve this now by paying a \$500 fine with a reloadable card, or we will need to send officers to your home today.”

What’s wrong here: courts contact prospective and missed jurors by mail, never by a phone call demanding immediate payment, and no law enforcement agency collects fines over the phone using a reloadable card. Scammers running this specific tactic sometimes provide real judges’ names and courthouse addresses to sound credible; those details don’t make the call legitimate. Hang up and, if concerned, contact your local court clerk’s office directly using a number you look up yourself.

Setting Up my Social Security Account

The Social Security Administration offers a free online account called my Social Security where you can view your benefit statements, request a replacement card in some cases and update direct deposit information. Setting

this account up yourself, proactively is one of the most protective things you can do, because it closes off a path scammers sometimes use: creating a fraudulent account in your name before you've claimed your own.

TRY IT YOURSELF Set Up My Social Security Account

Open your browser and type ssa.gov directly (do not search for it or click a link from an email).

Look for “my Social Security” and select “Create an Account.”

Follow the identity verification steps, which will ask questions only you would know the answers to.

Once set up, review your benefit statement and confirm your direct deposit information is correct.

Medicare Online

Medicare.gov offers a similar account system for reviewing your coverage, claims, and Part D prescription drug plan details. During Medicare's annual open enrollment period each fall, scam activity around fake plan changes tends to spike, since scammers know real mail and calls about plan options are

genuinely arriving during that window, giving cover for fraudulent ones to blend in. Any call claiming to require immediate payment or personal information to keep your current Medicare coverage active should be treated with the same skepticism covered in Chapter 4.

Filing Taxes and Avoiding IRS Scams

IRS impersonation scams have remained consistently common for years, largely because tax season creates genuine anxiety that scammers can exploit. It's worth knowing directly from the IRS's own guidance: the agency will first contact you by mail if there's a genuine issue with your taxes, not by phone, text, or email, and it will never demand immediate payment by gift card, wire transfer, or cryptocurrency, and never threaten immediate arrest over the phone.

SPOT THE SCAM The IRS Threat Call

"This is a final notice from the IRS. You owe \$4,800 in back taxes. A warrant has been issued for your arrest. To resolve this immediately, purchase gift cards and provide the numbers to avoid law enforcement being dispatched to your home."

What's wrong here: this message combines nearly every red flag from Chapter 4 at once: urgency, authority, an unusual payment method, and a threat. The IRS does not operate this way. Hang up. If you have any doubt about your actual tax status, look up the IRS's official number yourself and call them directly.

Choosing a Tax Preparer, You Can Trust

Beyond scam calls impersonating the IRS, a quieter but costly problem involves dishonest tax preparers themselves. The IRS specifically warns each filing season about what it calls “ghost preparers,” individuals who prepare a tax return for a fee but refuse to sign it or include their legally required Preparer Tax Identification Number, leaving the taxpayer solely responsible if the return turns out to be fraudulent. Ghost preparers often set up temporary offices around tax season, sometimes at a church, a community center, or another gathering place, and disappear afterward, along with any fee they charged.

A few warning signs are worth remembering when choosing anyone to prepare your taxes: a preparer who bases their fee on a percentage of your refund, one who promises an unusually large refund before ever reviewing your documents, or one who asks

you to sign a blank or incomplete return. By law, every paid preparer must sign the return they prepare and include their identification number; asking to see it and confirming the return they file matches what you reviewed together, is a reasonable and normal thing to request.

It's also worth knowing that new tax law changes, including recent additional deductions specifically for filers 65 and older, have created fresh opportunities for scammers to claim you need to "enroll" or "verify eligibility" for a benefit that applies automatically with no sign-up required. Any unexpected call, text, or email urging quick action to secure a tax benefit is worth treating with the same skepticism as the other IRS impersonation tactics in this chapter.

Medicare Open Enrollment: A High-Risk Season

Medicare's annual open enrollment period runs each year from October 15 through December 7, with a separate Medicare Advantage enrollment window running January 1 through March 31. Consumer protection agencies consistently report a sharp seasonal spike in Medicare-related scam calls and texts during these windows,

since scammers deliberately exploit the genuine flurry of real plan-comparison activity happening at the same time to make their fraudulent contact blend in.

One useful, official safeguard to know about: any licensed agent who wants to discuss specific Medicare plan options with you is required to have you sign a form called a Scope of Appointment beforehand, which limits the conversation to only the topics you agreed to in advance, and current rules require at least 48 hours between signing that form and the actual appointment in most cases. An agent who skips this step, or who pressures you to discuss additional products beyond what you agreed to, is not following Medicare's own rules, regardless of what they claim.

It's also worth knowing that federal investigators estimate Medicare loses tens of billions of dollars each year to fraud, waste, and improper payments, a scale that helps explain why the program invests heavily in beneficiary protection and why your own vigilance genuinely matters as part of that larger system, not just for your own benefit.

SPOT THE SCAM The New Card Text

A text message arrives from an unfamiliar short number: “Your new Medicare benefits card is ready. Click here to confirm your address and receive your \$2,600 senior benefits card before the deadline.”

What’s wrong here: Medicare does not initiate contact by text message, is not issuing new cards to all members, and has no program called a “senior benefits card” tied to a dollar amount like this. Delete the message without clicking anything, and if you’re ever unsure, call Medicare directly at 1-800-633-4227.

Renewing Licenses and Other State Services

Many state-level services, including driver’s license renewal, vehicle registration, and property tax payment, now offer online options through official state government websites, typically ending in “.gov”. That ending is a useful, though not perfect, signal: government websites are restricted to actual government agencies in a way that ordinary “.com” addresses are not. When in doubt about a state service, the safest starting point is searching for the agency’s name directly rather than clicking a link from an email or text claiming urgency.

Understanding Benefit Statements and Notices

Every year, the Social Security Administration and Medicare send official statements and notices, and it's worth developing the habit of reading them, since they establish a baseline for what genuine correspondence from these agencies looks like. Genuine Social Security mail includes your specific claim number and is printed on official letterhead; it never asks you to call a number to "verify" your Social Security number, since the agency already has that information on file. Familiarizing yourself with what real notices look like makes a fraudulent imitation far easier to spot by comparison.

If you ever receive a notice you're unsure about, whether by mail, phone, or email, the safest verification step is the same one repeated throughout this book: set the notice aside, and call the agency directly using a number you look up yourself, either from ssa.gov, medicare.gov, or irs.gov, or from a previous, trusted piece of mail, not from the notice in question itself.

The Difference Between Medicare Parts

Medicare can feel confusing partly because it's several distinct programs bundled under one name. Part A covers hospital stays. Part B covers doctor visits and outpatient care. Part D covers prescription drugs. Medicare Advantage, sometimes called Part C, is an alternative way of receiving your Part A and B benefits through a private insurance company, often bundling in extra benefits like dental or vision coverage. Understanding which parts, you're enrolled in helps you recognize when a call or letter about your "Medicare benefits" is referencing something that doesn't match your real coverage, a useful red flag.

Free, unbiased help navigating these choices is available through your State Health Insurance Assistance Program, commonly called SHIP, a federally funded counseling service with no connection to any insurance company selling a product, meaning counselors have no financial incentive to steer you toward a particular plan. This is worth knowing about specifically because many Medicare scams and aggressive sales tactics rely on people not knowing that free, neutral help exists.

Saving Money on Prescriptions

Beyond Medicare Part D coverage, several free tools can lower what you pay at the pharmacy counter, and it's worth knowing they exist even if you already have prescription coverage, since they sometimes beat your insurance price for a specific medication. Prescription discount services like GoodRx offer free coupons you show your pharmacist, comparing prices across nearby pharmacies for the same medication, which can vary surprisingly widely from one pharmacy to another for the exact same drug. These are legitimate, free tools, not insurance, and using one doesn't affect your actual insurance coverage.

Medicare's own Extra Help program provides additional prescription assistance for beneficiaries with limited income and resources, and many pharmaceutical manufacturers separately offer patient assistance programs for their specific brand-name drugs, worth asking your doctor's office or pharmacist about directly if a particular medication's cost is a strain.

TRY IT YOURSELF Compare a Prescription Price

Before your next pharmacy pickup, try

comparing prices:

1. Ask your pharmacist what the price would be with a discount coupon versus your insurance copay.
2. If using a discount app or site, search your medication's name plus your zip code.
3. Use whichever price is lower; you can typically choose either option at the counter.

CHECKLIST Government Services Check

- ☐ I know government agencies contact me by mail first, not by surprise phone call.
- ☐ I have set up, or plan to set up, my Social Security account directly at ssa.gov.
- ☐ I know Medicare and the IRS will never demand gift cards or wire transfers.
- ☐ I know to look for “.gov” when using state government websites.

MY NOTES

Chapter 9: Community Resources & Local Support

Staying safe and confident online is only part of navigating daily life well. This chapter turns outward, toward the community resources around you, many of which are free, underused, and specifically built with older adults in mind. Making this book a genuine, carry-along companion means it should help you find real help nearby, not just protect you from harm.

Your Local Library

Public libraries have quietly become some of the most valuable, and most overlooked, resources available to older adults navigating technology. Most libraries offer free computer and internet access, free one-on-one or small-group tech help sessions, and, increasingly, laptop or Wi-Fi hotspot lending programs for cardholders who don't have reliable service at home. Library staff are generally patient, knowledgeable, and glad to help with something as simple as setting up an email account or as involved as troubleshooting a new tablet.

TRY IT YOURSELF Find Your Local Library's Tech Help

Call or visit your nearest library branch and ask two questions:

1. Do you offer free computer or tech help classes, and how often?
2. Do you have a laptop or Wi-Fi hotspot lending program?

Write the branch name, address, and phone number in the space below.

MY NOTES

Senior Centers

Senior centers, sometimes called community centers for older adults, typically offer far more than social activities, though those matter too. Many provide congregate meals, transportation assistance, health screenings, exercise classes, and connections to benefits counselors who can help navigate Medicare, Medicaid, and other programs. In many areas, senior centers are also where programs like NAVIGATE are hosted, making them a natural

hub for both social connection and practical support.

Your local Area Agency on Aging, a federally supported network covering nearly every county in the country, maintains directories of senior centers and services in your specific area, and can typically be reached by calling the Eldercare Locator at 1-800-677-1116.

Researching Assisted Living and Aged Care Options

Whether for yourself or in support of a spouse or friend, researching assisted living or in-home care options can feel overwhelming. A few grounding questions help cut through the noise: Is the facility or agency licensed by the state? Can you tour in person, unannounced, rather than only on a scheduled showing? Are recent inspection reports available to review? What is the actual staff-to-resident ratio, not just the marketed one?

Every state maintains a Long-Term Care Ombudsman program, an independent advocate specifically tasked with protecting the rights of residents in nursing homes and assisted living facilities and investigating complaints. This office is worth knowing about and contacting with any concerns about

elder abuse or neglect, whether for yourself or someone you care about.

Transportation Help

Many communities offer senior-specific transportation programs, often free or low-cost, providing rides to medical appointments, grocery stores, and senior centers. Paratransit services, required by federal law in areas with public transit, offer door-to-door transportation for people who cannot use standard bus or rail service. Ride-hailing apps like Uber and Lyft also now offer simplified, phone-call-based booking options in some cities specifically designed for users who prefer not to navigate a smartphone app.

Food and Meal Support

Meals on Wheels, active in nearly every community nationwide, delivers meals directly to homebound older adults, often alongside a welcome daily check-in visit. Local food banks frequently offer senior-specific distribution days or home delivery options. SNAP, the federal food assistance program, has income eligibility limits that

surprise many people by being higher than they assume, so it is worth checking eligibility rather than ruling it out based on assumption alone.

Legal and Advocacy Resources

Free or low-cost legal aid for older adults is available in most areas, often through Legal Aid Society chapters or Area Agency on Aging partnerships, covering issues like estate planning, benefits appeal, and elder abuse. These resources exist specifically because legal problems disproportionately affect people who cannot afford standard legal fees, and eligibility is often based on age alone rather than income.

Planning for Your Digital Legacy

One topic rarely covered in a typical digital literacy program, but genuinely important, is what happens to your online accounts and digital information after you pass away or become unable to manage them yourself. Family members are frequently surprised to discover how difficult it can be to access a loved one's email, photos, or financial accounts afterward, since federal privacy law and individual companies' own rules often

prevent handing over access, even to a spouse or child, without advance planning.

A basic digital estate plan involves three things: a written inventory of your important accounts, a secure way for a trusted person to access them when needed, and a clear instruction for what you want done with each, whether that's closing an account, preserving photos, or transferring something of value. Financial and legal experts consistently advise against listing actual passwords directly inside a will, since a will often become a public court document after death; instead, a password manager with an emergency access feature, or a written list kept in a secure, separate location like a locked drawer or a safe deposit box, works better.

Many major platforms now also offer their own built-in legacy planning tools. Facebook allows you to name a "legacy contact" who can manage your profile after your passing. Google offers a similar tool called Inactive Account Manager, which can automatically notify a chosen person, and grant them limited access, if your account goes unused for a period you select. Setting these up takes only a few minutes and can spare your family significant difficulty later.

TRY IT YOURSELF Start Your Digital Inventory

On a sheet of paper, or in a notebook you'll keep somewhere secure, list:

1. Your most important accounts: email, banking, and any account holding photos you'd want preserved.
2. For each, a note of where the password is stored, not the password itself, if you're using a password manager.
3. The name of one trusted person who should be told where to find this list.

This is a good topic to raise directly with an estate planning attorney, particularly if you're already working on a will or power of attorney, since your digital plan should generally be coordinated with, though kept separate from, those formal legal documents. Free or low-cost legal aid for older adults, mentioned earlier in this chapter, can often provide guidance on this exact topic.

Faith Communities and Civic Organizations

Beyond formal government and nonprofit services, faith communities, whether a church, mosque, synagogue, or temple, often

serve as some of the most reliable and consistent sources of practical support for older adults, from organized visitation programs for homebound members to informal networks of people willing to help with rides or errands. Civic organizations, including groups like the Rotary Club, Lions Club, and local chapters of organizations such as AARP, frequently run their own volunteer programs specifically aimed at supporting older community members, sometimes including free tax preparation help, home safety checks, or technology tutoring like what NAVIGATE offers.

These informal networks are worth taking seriously alongside the more formal services listed elsewhere in this chapter, precisely because they often move faster and require less paperwork than government programs, even when they ultimately connect you to those same government resources.

Home Safety and Fall Prevention Resources

Falls are worth taking seriously as a safety topic, not just an inconvenience. The Centers for Disease Control and Prevention reports that more than one in four adults 65 and older falls each year, and falls remain the leading

cause of both fatal and nonfatal injury among older adults nationally, with roughly 3 million older adults treated in emergency departments for fall-related injuries annually. Perhaps most important for anyone living alone: research has found that when a fall isn't discovered for an hour or more, the risk to long-term health rises substantially, regardless of whether the fall itself caused a serious injury, simply because of the time spent unable to get up or call for help.

This is precisely the gap that medical alert devices are built to close. A basic medical alert system is a wearable button, often a pendant or wristband, that connects to a monitoring center at the press of a button. Many modern systems also offer automatic fall detection, using motion sensors to recognize the specific pattern of a fall and contact help even if the wearer is unable to press the button themselves. Despite how common falls are, national surveys suggest fewer than one in ten older adults currently uses this kind of safety technology, meaning it remains a significantly underused protection for most families.

Many Area Agencies on Aging and local fire departments offer free home safety assessments, a trained visitor who walks

through your home identifying fall risks, like loose rugs or poor lighting, and sometimes providing or installing simple safety equipment like grab bars at no cost. Given how much falls affect long-term independence, this is a genuinely valuable, and frequently underused, free resource worth actively seeking out rather than waiting to be offered.

Smart Speakers and Voice-Activated Help at Home

A standalone smart speaker, such as an Amazon Echo, Google Nest, or Apple HomePod, works entirely through spoken commands rather than a screen, which makes it one of the more approachable pieces of technology available to older adults, since it relies on a skill everyone already has: talking. National surveys from AARP have found that roughly three in ten adults 50 and older have already adopted a smart speaker of some kind, and that adoption has continued climbing steadily in recent years.

Beyond convenience, like asking for the weather or setting a timer while cooking, these devices offer genuine safety value. Many can be set up to call a family member, or in some cases emergency services, using only

a voice command, which matters enormously in a moment when reaching for a phone isn't possible, including after a fall. Medication reminder features, available on all three major platforms, can prompt you by voice at set times each day. For anyone managing hearing loss, features like Amazon's Alexa Captions can display spoken responses as on-screen text on a compatible device, and larger-screen versions of these speakers offer visual reminders alongside the voice ones.

Setting one up typically involves plugging it in, connecting it to your home Wi-Fi through a companion app on your phone, and a brief voice-guided setup. If the setup process itself feels intimidating, it's worth asking at your local library or senior center, covered earlier in this chapter, since tech help sessions increasingly include smart speaker setup as a common request.

Continuing Education and Lifelong Learning

Many community colleges and universities offer free or significantly discounted tuition for older adults, sometimes called senior audit programs, allowing you to sit in on college courses purely for the enjoyment of learning, without needing to complete assignments or

exams. Organizations like OLLI, the Osher Lifelong Learning Institute, operate specifically to offer courses, lectures, and social connection designed for adults over 50, often held at local universities. These programs are worth exploring not just for their educational value but because ongoing learning and social engagement are both associated with better long-term cognitive health.

Volunteering and Giving Back

Many older adults find that volunteering offers some of the same benefits as continuing education: structure, social connection, and a sense of purpose, alongside a genuine contribution to the community. RSVP, part of the national Senior Corps network, specifically matches volunteers 55 and older with local opportunities matched to their skills and interests, from mentoring students to supporting local nonprofits. Many of the organizations already mentioned in this chapter, libraries, senior centers, and faith communities, also rely heavily on volunteers and are often glad to have help from someone who understands, firsthand, what it's like to be on the receiving end of their services.

If technology itself is an interest, participants may go on to become informal tech mentors for newer NAVIGATE participants, or volunteer at library tech help sessions, turning a skill this book helped build into something shared with others.

Getting Help with Errands and Household Tasks

For tasks that become harder to manage alone, whether grocery shopping, yard work, or minor home repairs, a combination of community and paid resources can help. Many senior centers and religious congregations, both covered earlier in this chapter, run informal volunteer chore programs connecting older residents with help for small tasks, often at no cost. Paid task and errand apps, such as TaskRabbit, offer another option for one-off jobs, with reviews and background information about each worker visible before you hire them, like the vetting habits already covered for other online services in this book.

Whichever route you choose, the same general safety habits apply: verify any worker through reviews or an agency rather than someone who simply showed up at your door offering services, and never feel pressured to

make an on-the-spot payment or decision for home repair work, a common setting for the door-to-door scams sometimes targeting older homeowners specifically after storms or other visible damage in a neighborhood.

TRY IT YOURSELF Find It Near You

Take a few minutes to fill in what you find, so this page becomes personalized to your own area:

My nearest library branch:

My nearest senior center:

My local Area Agency on Aging phone number:

A transportation option I could use:

A Note for Adult Children and Caregivers

If you're reading this book alongside a parent, or helping them work through it, a few things are worth knowing. Most smartphones now offer a family sharing or account linking feature, allowing an adult child to help manage settings, approve purchases, or assist with troubleshooting remotely, with the older

adult's knowledge and consent, rather than requiring an in-person visit for every small issue. On an iPhone, this is called Family Sharing, found in Settings under the account holder's name. On Android, Google's Family Link offers similar functionality, though it's worth noting these tools are most marketed for parents managing children's devices, so some menu navigation and adaptation is needed to use them supportively with an older adult instead.

It's worth having an honest conversation about the right level of involvement before setting anything up. Some older adults want a family member to have ongoing visibility into their accounts as a safety net; others want to remain fully independent and only want help when they specifically ask for it. Both are entirely reasonable, and the conversation itself, done openly rather than assumed, tends to prevent the friction that can otherwise arise when a family member's help feels more like surveillance than support.

CHECKLIST Community Resources Check

- ☐ I know my nearest library's tech help hours.
- ☐ I know where my nearest senior center is located.

☐ I have the Eldercare Locator number saved:
1-800-677-1116.

☐ I know at least one transportation option
available to me.

Chapter 10: Social Media & Staying Connected Safely

Social media platforms like Facebook, Instagram, and others have become genuine lifelines for staying connected with family scattered across the country or the world, sharing photos of grandchildren, and rebuilding contact with old friends. They are also, unfortunately, a primary hunting ground for scammers, precisely because so much personal information tends to sit in plain view.

Privacy Settings, Explained

Most social media platforms default to open sharing when an account is first created, on the assumption that new users want maximum visibility. Adjusting these settings afterward is worth the ten minutes it takes, and it is not a one-time task; platforms periodically change their settings menus and sometimes quietly reset preferences after an update, so a periodic check is worthwhile.

TRY IT YOURSELF Audit Your Facebook Privacy Settings

Open Facebook and tap the menu (often three lines or your profile photo).

Go to Settings & Privacy, then Privacy Center or Privacy Checkup.

Set “Who can see your future posts” to Friends, not Public.

Review “Who can see your friends list,” and consider limiting it to Friends only.

Review your profile photo and cover photo visibility as well, since these are often public by default even when other settings are restricted.

What Not to Share, and Why

A general rule worth adopting treat information the way you would treat a spoken conversation with a stranger standing nearby. Posting that you’re currently on vacation, for instance, tells anyone watching, including people you’ve never met, that your home is empty. Posting a photo of a new credit card, a boarding pass, or a birthday cake with your exact birth date printed on its hands over small pieces of information that, combined, can be used to answer security questions or impersonate you elsewhere.

This connects directly back to Chapter 5: publicly posted videos and voice clips of yourself are also raw material for voice cloning. This is not a reason to stop posting entirely, since genuine connection is valuable

and worth protecting too, but it is worth being thoughtful about what is public versus visible only to confirmed friends and family.

CHECKLIST Who Can See This?

- ☐ I know whether my recent posts are set to Public or Friends only.
- ☐ I avoid posting that I'm currently away from home.
- ☐ I avoid posting my full birth date, address, or phone number publicly.
- ☐ I know how to check who is on my friends list before accepting a new request.

Understanding Algorithms and Your Feed

The specific posts and videos you see on social media are not simply shown in the order they were posted. Each platform uses a computer program, often called an algorithm, that selects and orders content specifically intended to keep you engaged and scrolling longer, based on what you've previously clicked, watched, or lingered on. This matters for two reasons. First, it explains why you might see an unusually large number of ads or posts related to something you searched for

once. Second, and more importantly for the purposes of this book, scammers have become adept at designing content specifically to perform well within these algorithms, meaning a fraudulent investment pitch or fake product ad can appear repeatedly and prominently, not because it's trustworthy, but because it's engineered to spread.

Understanding that your feed is curated by a program optimizing for your attention, not for accuracy or trustworthiness, is a useful piece of mental armor. Repetition and popularity on social media are not evidence that something is true or safe.

Marketplace and Buy-Sell Groups

Facebook Marketplace and similar buy-sell groups have become popular ways to buy and sell used items locally, and they are broadly safe when a few precautions are followed. Meeting in a public place, such as a police station's designated "safe exchange" parking area, many departments offer this specifically, is safer than inviting a stranger to your home or going to theirs. Never send payment in advance for a marketplace item and be skeptical of a seller or buyer who insists on shipping when the listing is local, or who suddenly needs to "complete the

transaction” through an unfamiliar payment link outside the platform itself.

One specific variation worth naming directly: pet scams. A listing shows an irresistible photo of a puppy or kitten, often a purebred, at a price that seems reasonable given how the breed usually sells. After a deposit is sent, the “breeder” invents additional fees, shipping costs, a special crate, travel insurance, before ever delivering the animal, which in most cases never existed at all. A legitimate breeder is willing to do a live video call showing the actual animal in real time, will let you visit in person before paying anything, and won’t pressure you toward an unusual payment method. If a seller has an excuse for every one of these requests, that pattern itself is the answer.

A common tactic involves a scammer copying a real friend’s public profile photo and name to create a duplicate, fake account, then sending friend requests to that person’s actual friends and family. Once accepted, the fake account may message asking for money, citing an emergency, counting on the request feeling legitimate because it appears to come from someone you already know and trust.

SPOT THE SCAM The Duplicate Friend Request

You receive a new friend request from someone who appears to already be your friend, using the same name and photo. A message soon follows: “Hey, it’s me, I got locked out of my old account, can you help me out with something small, I’m in a bind.”

What’s wrong here: if you’re already friends with someone, a second request from an identical-looking profile is a near-certain sign of impersonation. Don’t accept the new request. Instead, message or call your actual friend through your existing, original connection to confirm, and consider reporting the fake profile to the platform.

Sharing Photos Across the Family

Photo sharing has become one of the most rewarding uses of technology for many grandparents, and it’s worth knowing your options beyond posting publicly on social media. Apps like Google Photos and Apple’s Shared Albums let you create a private, invitation-only album that only specific family members can see and add to, which sidesteps the privacy tradeoffs covered earlier in this chapter entirely, since nothing in a shared

album is visible to the wider internet. Many families set up a running shared album for a new grandchild or great-grandchild, so new photos appear automatically for everyone invited, without anyone needing to remember to send them individually.

TRY IT YOURSELF Set Up a Shared Photo Album

On an iPhone: open Photos, tap the plus icon, choose “New Shared Album,” name it, and invite family members by their phone number or email.

On Android with Google Photos: open the app, tap the plus icon, choose “Album,” then “Share,” and select who to invite.

Ask a family member to help you create your first one if this feels unfamiliar; it only needs to be set up once.

Recognizing Online Harassment

Not everything unpleasant that happens online is a scam in the sense covered elsewhere in this book; sometimes it's harassment, meaning repeated, unwanted contact intended to upset, intimidate, or humiliate rather than to extract money. This can come from a stranger reacting to something you posted, or, less often, from

someone you know. Every major platform offers tools to block a specific person entirely, preventing them from contacting you or seeing your posts, and to report content that violates the platform's rules, both usually accessible from a small menu icon near the offending post or message.

You are never obligated to engage with or respond to harassment before blocking someone; blocking first and deciding whether to report afterward is a completely reasonable order of operations. If harassment includes threats of violence, it's worth taking a screenshot before blocking, since the content disappears from your view once blocked, and reporting the threat to local police, in addition to the platform itself.

Texting Like the Rest of the Family

Text messaging conventions have shifted over time in ways that can make family group chats feel like a foreign language at first. A few small things help close that gap. Emojis, the small pictures like a smiling face or a heart, are simply a fast way to express tone that can otherwise be lost in a short message; using a few is welcomed, not required, and there's no wrong way to use them. Abbreviations like "LOL" (laughing out loud) or "OMW" (on my

way) are common shortcuts younger family members use, and it's entirely fine to ask what one means rather than guessing.

Group chats, a single conversation thread involving several people at once, are worth understanding structurally: a message you send appears to everyone in the group, not just one person, which occasionally causes an accidental overshare. Most messaging apps let you leave a group chat or mute its notifications if it becomes overwhelming, found by tapping the group's name at the top of the conversation.

Staying Connected Through Video Calls

Video calling apps like FaceTime, Zoom, and WhatsApp allow face-to-face conversation regardless of distance, and are worth genuine comfort and practice, since seeing a loved one's face carries real emotional value that a phone call alone doesn't fully replace. Video calls are also, as covered in Chapter 5, one of the best real-time tools for confirming a person's identity, since a live, responsive video call is far harder for a scammer to fake convincingly than a recorded voice clip.

TALK ABOUT IT

Ask a family member to set up a regular video call day, even just once a month, and try it together this week if you haven't before.

MY NOTES

Chapter 11: Building Your Digital Confidence Score

Back in Chapter 1, you completed a short checklist and counted how many boxes you checked. That number was your starting Digital Confidence Score. Now that you've worked through the core material in this book, this chapter offers a fuller self-assessment, along with a way to set concrete goals for whatever gaps remain.

The Full Self-Assessment

Unlike the short version in Chapter 1, this assessment covers each major area from the book. Go through it honestly; the purpose is not a passing grade but an accurate picture of where you stand today, so you can decide where to focus next.

CHECKLIST Devices & Internet Basics

- ☐ I know how to check for and install updates on my device.
- ☐ I know how to check if a website connection is secure.
- ☐ I know how to identify who sent an email.

CHECKLIST Scam Recognition

- ☐ I can name the three ingredients common to most scams (urgency, authority, isolation).
- ☐ I know never to pay with gift cards or wire transfers to resolve a supposed emergency.
- ☐ I have a rehearsed pause phrase I use when something feels urgent.
- ☐ My family has agreed on a safe word for genuine emergencies.

CHECKLIST Banking & Healthcare

- ☐ Two-factor authentication is turned on for my bank and email.
- ☐ I check my bank account activity at least weekly.
- ☐ I have access to, or a plan to set up, a patient portal account.

CHECKLIST Government & Community

- ☐ I have my Social Security account, or a plan to set one up.
- ☐ I know my nearest library and senior center.
- ☐ I know at least one transportation resource available to me.

CHECKLIST Social Media

- ☐ My social media privacy settings are reviewed and set the way I want them.
- ☐ I know how to recognize a duplicate or fake friend request.

Why Scoring Yourself Honestly Matters

There can be a temptation, particularly the second time through a self-assessment like this, to check boxes based on what you know you should be doing rather than what you are doing. Resist that temptation. This assessment has no audience but you, and an honest, lower score that accurately reflects reality is far more useful than an inflated one that leaves real gaps quietly unaddressed. The NAVIGATE model is designed to encourage participants to be candid about their remaining gaps, because identifying those gaps helps focus subsequent practice.

Understanding Score Plateaus

It's common to see rapid improvement in your Digital Confidence Score early on, followed by a plateau where progress feels slower. This is a normal part of any learning process, not a

sign that you've stopped improving. The early gains often come from the most visible, structural changes covered in this book, like turning on two-factor authentication or setting up your Social Security account. The later gains, developing the instinct to pause automatically when something feels off, or becoming genuinely comfortable rather than merely capable with a device, take longer to settle in, because they depend on repeated real-world practice rather than a single setting you can switch on.

If you find yourself plateaued, it can help to revisit a specific chapter you found most difficult and work through its "Try It Yourself" activity again, rather than pushing forward into new material. Depth in a few areas is often more protective than shallow familiarity with everything.

Measuring Progress Together

Digital confidence tends to build faster in a group than alone, which is part of why NAVIGATE is designed as a cohort program rather than a set of individual lessons. Hearing another participant describe the same confusion you felt, or the same scam call you nearly fell for, normalizes the experience in a way reading about it in a book alone

cannot fully replicate. If you're working through this book outside a formal NAVIGATE session, consider finding even one other person, a neighbor, a friend, a family member, to compare notes with as you go.

Progress also looks different for different people, and that's worth naming directly. For one reader, success might mean feeling calm the next time an unexpected call comes in. For another, it might mean finally feeling ready to manage banking online independently. Both are real, meaningful progress, and neither is more valid than the other.

A 30-Day Practice Plan

If you'd rather work through this book with real structure instead of reading straight through, here is one way to pace it, roughly matching the six NAVIGATE sessions with time in between to practice. Adjust freely; the point is steady, repeated practice, not speed.

Days 1-5: Read Chapters 1 through 3. Complete the device labeling and email practice activities.

Days 6-10: Read Chapters 4 and 5. Choose your pause phrase and set up a family safe word.

Days 11-15: Read Chapter 6. Turn on two-factor authentication for your bank and email.

Days 16-20: Read Chapters 7 and 8. Set up or confirm access to your patient portal and my Social Security account.

Days 21-25: Read Chapters 9 and 10. Complete the “Find It Near You” worksheet and review your social media privacy settings.

Days 26-30: Read Chapters 11 through 14. Complete your full self-assessment and fill in your Emergency Action Plan.

Setting Goals for What’s Left

Nobody finishes this book with every single box checked immediately, and that’s expected. What matters is identifying two or three specific, achievable next steps rather than feeling you must master everything at once.

TRY IT YOURSELF My Next Three Steps

Looking back over the checklists above, write down the three items that feel most worth tackling next:

1. _____
2. _____
3. _____

Consider bringing this list to your next NAVIGATE session for support in working through it.

Revisit this chapter every few months. Technology changes, scam tactics evolve, and your own comfort will keep growing the more you practice. A Digital Confidence Score is not a final grade; it's a snapshot you're allowed, and encouraged, to keep retaking.

MY NOTES

Chapter 12: What to Do If You've Been Scammed

If you're reading this chapter because something has already happened, the most important thing to know is this: you are not alone, this is not your fault, and acting quickly genuinely improves your chances of recovering money and limiting further damage. Shame and embarrassment are extremely common reactions, and they are also exactly what keeps many scams from ever being reported, which only helps the people committing them. Reporting what happened, even if it feels difficult, protects both you and others who might otherwise face the same scheme.

Immediate Steps

The first hour after realizing something is wrong matters most. If you've shared account information, passwords, or made a payment, act on the following steps in roughly this order, adjusting based on what happened to you.

1. Stop all contact. Do not respond further, do not send additional payment even if threatened, and do not engage to reason with the scammer.

2. Call your bank or card company immediately. Use the number on the back of your card, not one given to you by the scammer. Ask them to freeze or reverse any transaction and to watch your account closely.
3. Change your passwords. Start with your email and banking passwords if any account information was shared, then any other account using the same or a similar password.
4. Tell someone you trust. A family member, friend, or your NAVIGATE facilitator can help you think clearly and take the next steps, which is much harder to do alone while still feeling shaken.

Reporting the Scam

Reporting serves two purposes: it may help recover your specific loss, and it feeds into a larger system that tracks scam patterns and occasionally leads to arrests. Reports should generally go to several places, since each agency handles a different piece.

The Federal Trade Commission, at reportfraud.ftc.gov, is the general clearinghouse for consumer fraud reports of nearly any kind. The FBI's Internet Crime Complaint Center, at ic3.gov, specifically

handles internet-based crimes, including romance scams and tech support fraud. If money was wired or sent through a specific service like Western Union or a gift card company, that company's own fraud department should also be contacted directly and promptly, since some have limited windows during which a transaction can potentially still be stopped.

It's worth understanding what happens after a report is filed, since the process rarely feels as immediate or satisfying as reporting a lost wallet. The FTC and FBI aggregate reports across thousands of victims to identify patterns and build cases against organized fraud operations, a process that can take months or years and does not always result in a call back to you personally. This can feel discouraging, but it does not mean your individual report was wasted; large-scale takedowns of scam operations are almost always built from the accumulation of many individual reports, including ones that felt, at the time, like they disappeared into the void.

Filing a Local Police Report

In addition to federal reporting, it's worth filing a report with your local police department, even though local police typically

cannot pursue an overseas scam operation directly. A police report creates an official record that can be required by your bank, your insurance company, or the credit bureaus as part of recovering funds or clearing fraudulent accounts opened in your name. Bring any documentation you have, screenshots of messages, transaction records, phone numbers involved, since a well-documented report is handled more efficiently than a vague one.

TRY IT YOURSELF Documenting What Happened

Whether for a police report, a bank dispute, or your own records, write down what you remember while it's fresh:

What happened (a few sentences, in your own words): _____

Date and time it started: _____

Phone numbers, email addresses, or website names involved: _____

Amount of money involved, if any:

Payment method used (card, wire, gift card, other): _____

Screenshots or messages saved? Where:

If Personal Information Was Exposed

If you shared your Social Security number, it is worth placing a free fraud alert or credit freeze with the three major credit bureaus (Equifax, Experian, and TransUnion), which makes it harder for anyone to open new credit in your name. The Social Security Administration's own fraud reporting line, and IdentityTheft.gov, a federal resource, can also walk you through a personalized recovery plan based on exactly what information was exposed.

Should You Pay for Identity Theft Protection?

You may see advertisements for paid identity theft protection services, such as LifeLock or IdentityForce, typically costing anywhere from about 10 dollars to nearly 30 dollars a month. It's worth understanding what these services offer versus what's already available to you for free, so this is a decision you make with clear information rather than out of fear.

This is a genuine financial choice, not something with a single correct answer for everyone, and it isn't legal or financial advice, just the facts to weigh.

A credit freeze, covered in Chapter 6, is entirely free and directly prevents new credit from being opened in your name, which is the single most damaging outcome of identity theft. You're also entitled to a free credit report from each of the three bureaus at least once every twelve months through the official site, annualcreditreport.com, which you can space out across the year to check your credit repeatedly at no cost. What a paid service typically adds beyond this is broader monitoring, such as watching the dark web for your information, tracking public records, and, in more comprehensive plans, dedicated recovery staff who handle much of the paperwork on your behalf if theft does occur, along with insurance covering certain out-of-pocket recovery costs.

Whether that added convenience is worth the ongoing monthly cost depends on your own comfort managing the free tools yourself, and how reassured you'd feel by dedicated recovery support if something ever did go wrong. If you do consider a paid service, it's worth reading the specific plan details

carefully rather than the advertisement alone, since coverage and included features vary considerably between providers and between tiers of the same provider.

Emotional Recovery Matters Too

Financial recovery is only part of what happens after a scam. Many people describe a real sense of violation, embarrassment, or grief, particularly with romance scams where a genuine emotional bond, even if built on a lie, was involved. These reactions are completely normal, and speaking with a counselor, a trusted faith leader, or a support group specifically for scam survivors can be genuinely valuable. Your local Area Agency on Aging, mentioned in Chapter 9, can often point you toward this kind of support as well as the practical, financial kind.

It can also help to remember that recovery, in the emotional sense, is rarely linear. Anger, embarrassment, and even a lingering distrust of technology or of people in general are all common in the weeks following a scam, and they tend to ease gradually rather than all at once. Returning to this book and to your NAVIGATE group during that period, rather than withdrawing from technology altogether, is itself part of a healthy recovery, since

isolation tends to prolong distress rather than resolve it.

Helping Someone Else Who Has Been Scammed

If a family member or friend confides in you that they've been scammed, the way you respond matters enormously to whether they come to you again in the future, or whether they hide it out of fear of judgment. Avoid leading with questions like "how could you fall for that" or "I told you this would happen," even if those thoughts cross your mind. Instead, lead with reassurance: this happens to smart, careful people, and the priority right now is stopping further harm, not assigning blame. Judgment offered in that first vulnerable moment tends to close a door that is very hard to reopen later.

What Recovery Actually Looks Like Over Time

It can help to know roughly what to expect in the weeks after reporting a scam, since the process rarely resolves as quickly as people hope. In the first few days, your bank or card company will typically confirm whether a disputed charge can be reversed, which is often the fastest-moving part of the whole

process. Credit bureau freezes and fraud alerts take effect quickly, usually within a day of your request. Federal reports filed with the FTC or FBI, by contrast, often show no visible movement for weeks or months, since they're being aggregated into larger investigations rather than handled one case at a time.

If money was wired, sent through a gift card, or moved through cryptocurrency, it's important to know honestly that full recovery is often not possible, even with prompt reporting, since these payment methods were specifically chosen by the scammer for exactly that reason. This isn't a failure on your part or on the part of the agencies you've reported to; it's a hard limitation of how those payment systems work. Reporting still matters immensely, both for any partial recovery that might be possible and for the larger pattern it helps investigators build, but it's fair to hold realistic expectations about timeline and outcome from the start, rather than being blindsided by them later.

TRY IT YOURSELF Your Emergency Action Plan

Fill this in now, while calm, so it's ready if you ever need it:

My bank's fraud number: _____

My credit card's fraud number: _____

A family member or friend I would call first:

The FTC reporting site: reportfraud.ftc.gov

MY NOTES

Chapter 13: Emergency & Important Contacts

Keep this section handy, whether by folding down the corner of this page, photocopying it, or taking a photo of it with your phone. It gathers the numbers most likely to matter in an emergency or a moment of doubt, drawn from every chapter in this book, in one place.

A word on how to use this chapter well: the categories below are organized by what kind of help you need, not by how urgent it feels in the moment, since panic can make any of these situations feel like an emergency even when it isn't one requiring 911. If you're ever unsure which category fits, start with Fraud & Scam Reporting, since the FTC and FBI resources listed there can point you toward the right next step regardless of the specific situation.

Emergencies

Call 911 for anything involving immediate danger to life, health, or safety. Poison Control is staffed around the clock, even for concerns that turn out to be minor.

Police, Fire, Medical	911	Any immediate danger
--------------------------	-----	-------------------------

Emergency		
Poison Control	1-800-222-1222	24 hours

Fraud & Scam Reporting

Use these regardless of whether money was lost; a report of an attempt still helps investigators track patterns.

FTC Fraud Report	reportfraud.ftc.gov	General consumer fraud
FBI Internet Crime Center	ic3.gov	Online scams, romance scams
Elder Fraud Hotline (DOJ)	1-833-372-8311	Free, staffed by case managers

Financial

Contact these if your Social Security number or account information may have been exposed, covered in Chapter 6 and Chapter 12.

Equifax	1-888-298-0045	Credit freeze/fraud alert
Experian	1-888-397-	Credit

	3742	freeze/fraud alert
TransUnion	1-800-680-7289	Credit freeze/fraud alert
IdentityTheft.gov	identitytheft.gov	Federal recovery plan

Government

Use these numbers to verify any call or letter claiming to be from these agencies, covered in Chapter 8.

Social Security Administration	1-800-772-1213	Also ssa.gov
Social Security Fraud Hotline	1-800-269-0271	Report SSA impersonation
Medicare	1-800-633-4227	Also medicare.gov
IRS	1-800-829-1040	Verify tax notices

Community & Aging Services

Your starting point for nearly any local question, from senior centers to suspected financial exploitation, covered in Chapter 9.

Eldercare Locator	1-800-677-1116	Find local senior services
Adult Protective Services	(via Eldercare Locator)	Report suspected exploitation
Long-Term Care Ombudsman	(local, via Eldercare Locator)	Care facility concerns

My Personal Contacts

Fill in your own frequently needed numbers below.

My bank's fraud line		
My doctor's office		
My pharmacy		
Family member		

#1		
Family member #2		
NAVIGATE facilitator		

Chapter 14: Quick-Reference Appendix

Glossary

App: a program on your phone or tablet for a specific task.

Browser: the app used to visit websites (Safari, Chrome, Edge).

Cloud: internet-based storage for your photos and files, reachable from any of your devices.

Cookie: a small piece of tracking data a website uses to remember your activity, often for advertising.

Credit freeze: a free service that blocks new credit accounts from being opened in your name.

Deepfake: an artificially generated fake photo, video, or audio of a real person.

Passphrase: a strong password made of several unrelated words strung together.

Password manager: a tool that generates and remembers a unique password for each of your accounts.

Patient portal: a secure website or app for viewing your own medical records (e.g. MyChart).

Phishing: a fake message designed to trick you into giving up personal information.

Telehealth: a medical appointment conducted over video call rather than in person.

Two-factor authentication (2FA): a second security step beyond a password, usually a code sent to your phone.

URL: a website's address, shown in the browser's address bar.

Wi-Fi: a wireless connection to the internet.

Wire transfer: an electronic money transfer that is fast and very difficult to reverse once sent.

Frequently Asked Questions (FAQs)

Can a scammer access my device just by calling me? No. Simply answering a phone call or receiving a text cannot give anyone access to your device. Access typically requires you to click a link, download something, or grant remote access yourself, often after being talked into it.

Is it safe to give my card number over the phone? Only if you initiated the call to a number you looked up yourself. Never provide payment information to someone who called or texted you first.

What if I already gave a scammer my Social Security number? Visit [IdentityTheft.gov](https://www.identitytheft.gov) right away for a personalized recovery plan and place a credit freeze with all three credit bureaus, covered in Chapter 6.

Will I get in trouble for reporting a scam that I fell for? No. You are the victim of a crime. Reporting agencies exist to help you and to investigate the people responsible, never to penalize you.

How do I know if a text message is really from my bank? When in doubt, don't click anything in the text. Open your banking app directly, or call the number on your card, to check for yourself.

Is it too late for me to learn this if I've avoided technology for years? No. Every skill in this book is designed to be learnable starting from every possible level of prior experience, including none.

The Red Flags Checklist (Tear-Out)

CHECKLIST Before You Act, Ask

- ☐ Did I initiate this contact, or did it come to me unexpectedly?
- ☐ Am I being pressured to act immediately?
- ☐ Am I being asked to pay by gift card, wire transfer, or cryptocurrency?
- ☐ Am I being told to keep this a secret?
- ☐ Would a trusted family member agree this seems safe?

Troubleshooting FAQ

My device is running slowly. Restart it, check for pending updates, and check available storage space.

I forgot my password. Look for “Forgot Password” on the login screen; most services send a reset link to your email or a code to your phone.

I think I clicked a scam link. Don’t enter any information on the page it opened. Close the browser, run a security scan if your device offers one, and change your passwords as a precaution.

I don’t recognize a charge on my statement. Call your bank’s fraud line, listed in Chapter 13, right away.

My email is sending messages I didn’t write. Change your email password immediately from a different, trusted device, and turn on two-factor authentication if it isn’t already on. Your account has likely been accessed by someone else.

A website looks slightly different than usual. Check the address bar carefully for a misspelled or altered web address before entering any information. When in doubt, close the page and type the address yourself.

I can’t remember which chapter covered something. Use the Table of Contents at the

front of this book, or the glossary above, which lists many topics by keyword.

Finding Help in Your State

Beyond the national numbers in Chapter 13, every state also maintains its own consumer protection office, typically housed within the state Attorney General's office, which handles complaints specific to state law and can be a useful additional resource alongside the federal agencies covered throughout this book. A web search for "[your state] Attorney General consumer protection" will lead you to the correct office, or your local library or senior center, covered in Chapter 9, can help you find and write down the right number for where you live.

MY NOTES State Resources I've Found

What's Changed Since This Book Was Printed

Every specific tool, app, and scam tactic named in this book will eventually be replaced by a newer version of the same underlying

pattern; that's true of any book about technology, and it isn't a reason to worry that this one will quickly become useless. The principles running through every chapter, pausing before you act, verifying independently, treating urgency and secrecy as warning signs, and knowing where to turn for help, don't expire the way a specific app or phone number might.

If something in this book ever feels out of date, that's worth bringing to a NAVIGATE session or a conversation with your local library, both covered in Chapter 9, rather than a reason to set the book aside. Technology will keep changing. The habits in this book are built to change with it.

About the Author

Nana Sarfo Brobbey is the founder of Brobbs Connect, a community technology practice based in Anaheim and Santa Ana, California. Brobbs Connect is built around NAVIGATE, a digital literacy and fraud-protection program for adults 60 and older and GROUNDWORK, a digital foundation and community engagement program for at-risk youth.

Nana was born and raised in Ghana, where caring for older relatives was woven into everyday family life. After relocating to Southern California, he began developing a curriculum to help older adults navigate an increasingly digital world, which led to the creation of NAVIGATE and, later, this book.

About Brobbs Connect & NAVIGATE

Brobbs Connect is a community technology practice built around two programs: NAVIGATE, a six-session digital literacy and fraud-protection curriculum for adults 60 and older, and GROUNDWORK, an eight-session digital foundation program for youth.

NAVIGATE sessions are designed to cover everything in this book in a live, guided format, with a companion app and a Digital Confidence Score tool to track your progress alongside your facilitator and fellow participants.

To find out more about the sessions or to learn more, visit <https://brobbsconnect.dev> and <https://app.brobbsconnect.dev>.

Acknowledgments

This book is shaped by a lifetime spent around older adults, starting with the caregiving woven into daily life in Ghana, and continuing through years of helping a mostly older customer base navigate digital tools there. It's dedicated to the participants who will one day work through these pages together in a NAVIGATE session.

CERTIFICATE OF COMPLETION

This certifies that

has completed Navigate: A Digital Guide for
Older Adults

Date: _____

MY DIGITAL SAFETY PLEDGE

Fill this in as a personal commitment to yourself, once you've worked through the book.

I will pause before I click and give myself permission to slow down when something feels urgent.

I will verify independently, using a number or address I find myself, not one given to me by a caller or message.

I will ask, without embarrassment, when something feels unfamiliar or confusing.

I will talk with my family about scams openly, before an emergency, not just after one.

I will keep this book close and come back to it whenever I need to.

Signed: _____

Date: _____

Tell Us Your Story

Brobbs Connect would love to hear from you, whether it's a question this book didn't answer, a scam attempt you spotted using what you learned, or feedback on how to make this book better for the next reader.

Reach out through brobbsconnect.dev or bring your story to your next NAVIGATE session.

Notes

Notes

Note

