A PLAIN-ENGLISH PRACTICAL GUIDE

Keeping Your Phone Safe and Healthy

Simple Habits for iPhone and Android



Updates, Backups, Privacy, Scam Texts and Battery Care for iPhone and Android

Andrew Dominguez

Trinfinity Enterprises

Keeping Your Phone Safe and Healthy

Updates, Backups, Privacy, Scam Texts and Battery Care for iPhone and Android

Andrew Dominguez

Trinfinity Enterprises

Keeping Your Phone Safe and Healthy: Updates, Backups, Privacy, Scam Texts and Battery Care for iPhone and Android

Copyright 2026 by Andrew Dominguez.

Free to download. All rights reserved.

No part of this book may be reproduced, distributed, or transmitted in any form or by any means without written permission from the publisher, except for brief quotations in reviews. You are welcome to download this book and read it for free at trinfinityenterprises.com.

Independently published. First edition, 2026.

Trinfinity Enterprises, Dayton, Nevada.

Questions and corrections: andrew@trinfinityenterprises.com

Please read before you use this book. This book is for general information and education only. It is not legal, medical, financial, tax, or other professional advice, and reading it does not create a professional relationship of any kind. Laws, rules, prices, and research change, and every situation is different. Before you act on anything in this book, check it against current sources and talk with a lawyer, doctor, licensed professional, or other qualified expert as your situation calls for. I worked hard to get the facts right, but I can't promise that every detail is complete, correct, or current. You use this information at your own risk. To the fullest extent the law allows, Andrew Dominguez, Trinfinity Enterprises, and Andrew Dominguez's heirs, estate, successors, and assigns accept no responsibility or liability for any loss, injury, or damage of any kind that comes from using or relying on this book.

Contents

Before You Begin....1
Chapter 1: Know Your Phone....2
Chapter 2: Keep It Updated....4
Chapter 3: Back It Up....6
Chapter 4: Lock It Down....8
Chapter 5: Apps and Privacy....10
Chapter 6: Scam Texts and Calls....13
Chapter 7: Protect Your Phone Number....15
Chapter 8: Battery Care....17
Chapter 9: If Your Phone Is Lost or Stolen....19
Monthly Phone Check....22
My Phone Numbers....23
Where to Get Help....24
Acronyms....25
Sources....26
About This Book....27

Before You Begin

Most of us carry our bank, our photos, our email and our contacts in one small device. A phone that is kept up to date, backed up and locked is hard to break into and easy to replace. A phone that is not can cost you money, your pictures and a lot of time.

This short guide covers the habits that matter most for both iPhone and Android phones: updates, backups, the lock screen, app permissions, scam texts, protecting your phone number, battery care, and what to do when a phone is lost or stolen. It is a companion to Keeping Your Windows PC Healthy, which covers the same ground for a home computer.

How to Use This Book

Each chapter gives the steps for iPhone first, then Android. Menu names were checked against Apple and Google support pages as of November 18, 2026. Android phones are made by many companies, and Google's own pages say menus and update schedules vary by device, maker and carrier. If a menu on your phone looks different, open Settings and use the search box at the top.

The appendix has a monthly phone check and a page to write down the numbers you need if your phone is ever lost.

What This Book Is and Is Not

This is general information for everyday phone owners. It is not technical support for a specific phone. For help with your phone, go to Apple Support, Google's Android Help, your phone's maker, or your wireless carrier.

Chapter 1: Know Your Phone

Before you change any settings, take two minutes to learn what you have. You will need these details when you call for help, check for updates, or report a lost phone.

iPhone

Open Settings, then General, then About. This screen shows your phone's model name, the version of iOS it runs, and its serial number. Write the model and serial number on the page at the back of this book.

Android

Open Settings, then About phone. Google's Android Help says this screen shows your Android version, your Android security update date, your Google Play system update, and the build number. The security update date tells you how current your protection is. If that date is many months old, your phone may need an update, or it may be too old to get them.

Your Accounts

Every phone is tied to an account. An iPhone uses an Apple Account. An Android phone uses a Google Account. That account holds your backups, finds a lost phone, and lets you set up a new one. If you lose the password to that account, you can lose all of it.

- Know the email address your phone account uses.
- Use a strong password for that account that you do not use anywhere else.
- Keep your recovery phone number and email up to date in the account settings.

- Write down where you keep the password. Do not write the password itself in this book.

Checklist

- ☐ I know my phone model and system version.
- ☐ I know which email my Apple or Google Account uses.
- ☐ My account recovery phone and email are current.

Chapter 2: Keep It Updated

Updates fix security holes that criminals already know about. An out-of-date phone is the easiest kind to break into. Turning on automatic updates is the single best thing most people can do.

iPhone

Apple's update page lists three steps to take before updating: back up your phone, plug it into power, and connect to Wi-Fi.

1. Open Settings, then General, then Software Update.
2. The screen shows the iOS version you have and whether an update is ready.
3. If one is ready, tap Download and Install and follow the steps on the screen.

To turn on automatic updates, go to Settings, then General, then Software Update, then Automatic Updates. With Automatically Install turned on, Apple says the phone installs updates overnight while it is charging and on Wi-Fi, and lets you know before it installs.

If the phone says there is not enough space, Apple says you can tap Continue to let it remove some apps for a short time. They are put back automatically after the update. You can also tap Cancel and delete things yourself.

If an update never shows up on the phone, Apple says you can update it from a computer instead.

Android

1. Open Settings, then System, then Software updates. On some phones the menu has a different name; search Settings for “update.”
2. The screen shows whether an update is ready. Follow the steps on the screen.

Google’s Android Help says to connect to Wi-Fi and charge the phone to at least 75 percent before a big update. If a download stops, the phone tries again over the next few days. Google says most system updates and security patches install automatically, and that update schedules vary by device, maker and carrier.

Update Your Apps Too

Apps get security fixes as well. On an iPhone, apps update from the App Store. On Android, they update from the Google Play Store. Leave automatic app updates on in each store’s settings.

When a Phone Gets Too Old Google notes that older devices can’t always run newer versions of Android, and the same is true of older iPhones. A phone that no longer gets security updates still works, but it is less safe each month. If you bank or shop on your phone, plan to replace it once updates stop.

Checklist

- ☐ Automatic system updates are on.
- ☐ Automatic app updates are on.
- ☐ I checked for an update this month.

Chapter 3: Back It Up

Phones get dropped, drowned, lost and stolen. A backup turns that from a disaster into an errand. With a current backup, you can sign in on a new phone and have your contacts, photos, messages and settings back.

iPhone: iCloud Backup

To turn on automatic backups, Apple's steps are:

1. Open Settings and tap your name.
2. Tap iCloud, then iCloud Backup.
3. Make sure Back Up This iPhone is turned on.

Apple says the automatic backup runs when the phone is plugged in, on Wi-Fi, and locked. Most phones meet all three overnight.

To make a backup right now, go to the same iCloud Backup screen and tap Back Up Now. Stay on Wi-Fi until it finishes. The date and time of the last backup show under the button. Check that date once a month.

If you get a message that there is not enough iCloud storage, Apple's page says you can follow the steps on the screen to buy more. You can also back up an iPhone to a computer.

Android: Backup by Google

Google's Android Help gives these steps, though menu names vary by phone:

1. Open Settings, then Google (on some phones, Google services), then All services.
2. Tap Backup, or Backup and restore.

3. Make sure backup is turned on, then tap Back up now.

Google says each Google Account comes with up to 15 GB of free storage, and you can buy more through Google One. The backup covers apps and app data, call history, contacts, device settings, and text messages. Photos and videos are backed up through Google Photos.

Google also says to protect your backup by using a PIN, pattern or password to lock your phone, not just a swipe.

Restoring to a New Phone

On both kinds of phones, you restore during setup: you sign in with the same Apple or Google Account and choose the backup. Google says a full restore can take up to 24 hours, and that you cannot restore a backup from a newer Android version onto a phone with an older one.

> **Test It Before You Need It** Once in a while, open the backup screen and look at the date of the last backup. If it is more than a few days old, something is wrong. The most common causes are a full storage plan or a phone that is never left on Wi-Fi and the charger at the same time.

Checklist

- ☐ Automatic backup is turned on.
- ☐ My last backup date is recent.
- ☐ I know which account my backup is saved to.

Chapter 4: Lock It Down

A lock screen is the front door of your phone. Without one, anyone who picks it up can open your email, reset your passwords and read your texts.

Use a Real Passcode

Use a passcode, PIN, pattern or password, plus Face ID, Touch ID or a fingerprint if your phone has it. A swipe is not a lock. Google's backup page says to use a PIN, pattern or password to protect your backup, not a swipe. Pick a code that is not your birthday, your address or 1234, and do not share it.

Turn On Find My (iPhone) or Find Hub (Android)

This is what lets you find, lock or erase a lost phone. Turn it on now. It cannot be turned on after the phone is gone.

- iPhone: Open Settings, tap your name, then Find My, and make sure Find My iPhone is on.
- Android: Google's Android Help says Find Hub is on by default once you add a Google Account. A PIN, pattern or password is needed for the Find Hub network to help locate the phone.

iPhone: Stolen Device Protection

Apple added Stolen Device Protection in iOS 17.3. It protects you if a thief watches you type your passcode and then takes the phone. Apple's page says it needs two-factor authentication on your Apple Account, a passcode, Face ID or Touch ID, Find My, and Significant Locations turned on.

To turn it on, go to Settings, then Face ID and Passcode, enter your passcode, and turn on Stolen Device Protection. It may already be on.

When the phone is away from familiar places like home or work, Apple says it requires Face ID or Touch ID, with no passcode fallback, for things like using saved passwords, using saved cards in Safari, and erasing the phone. Changes to your Apple Account password and security settings, or to the passcode, also wait one hour and then ask for Face ID or Touch ID again.

Before You Sell or Trade In an iPhone Apple says to turn off Stolen Device Protection before you sell, give away or trade in the phone. Back it up first, then sign out of your Apple Account and erase it.

Android: Theft Protection

Many Android phones have theft and lost-device settings. Google's Find Hub page points to Settings, then Security and privacy, then Lost device protection or Theft protection, on Android 12 and later. Names vary by maker. Search Settings for "theft."

Checklist

- ☐ My phone has a passcode, PIN or pattern, not a swipe.
- ☐ Find My or Find Hub is on.
- ☐ Stolen Device Protection (iPhone) or theft protection (Android) is on.

Chapter 5: Apps and Privacy

Every app asks for permission to use parts of your phone: your location, camera, microphone, contacts or photos. Many apps ask for more than they need. A few minutes in Settings shows you who has what.

iPhone

Apple's privacy page gives these paths:

- Location: Settings, then Privacy and Security, then Location Services. Each app is listed, and you can tap it to change its permission. Apple says Allow Once gives access for one session only, and While Using the App limits it to when the app is in use.
- Everything else: Settings, then Privacy and Security, then pick a category such as Contacts, Photos, Microphone, Camera, Bluetooth or Health. Apple notes that an app only shows up in a category after it has asked for that permission.
- To start over, Settings, then General, then Transfer or Reset iPhone, then Reset, then Reset Location and Privacy. Apps will ask again before they use your location.

Android

Google's Android Help gives these paths, though names vary by maker:

- One app at a time: Settings, then Apps, then the app (or See all apps), then Permissions. Choose Allow or Don't allow.
- For location, camera and microphone, the choices are All the time (location only), Allow only while using the app, Ask every time, and Don't allow.

- One permission at a time: Settings, then Security and privacy, then Privacy, then Permission manager.
- Apps you never use: Settings, then Apps, then the app, and turn on Pause app activity if unused.

A Simple Rule

Ask yourself whether the app needs the permission to do its job. A map app needs your location while you use it. A flashlight app does not need your contacts. When in doubt, choose “while using the app” or “ask every time,” not “always.”

Only Install Apps From the Official Store

Get apps from the App Store on an iPhone or the Google Play Store on Android. Do not install an app because a text, email or caller tells you to.

On Android, Google Play Protect checks apps for harm. Google says it is on by default and recommends you always keep it on. To check, open the Play Store, tap your profile picture, then Play Protect, then Settings, and make sure Scan apps with Play Protect is on. If it finds a harmful app, the alert gives you a way to uninstall it.

Delete What You Do Not Use

Old apps can still collect data and may stop getting fixes. Once a year, scroll through your apps and delete the ones you have not opened in months.

Checklist

☐ I reviewed which apps use my location.

☐ I reviewed camera, microphone, contacts and photos access.

☐ I deleted apps I do not use.

☐ Play Protect is on (Android).

Chapter 6: Scam Texts and Calls

The Federal Trade Commission (FTC) says scammers send fake texts to get your password, account numbers or Social Security number. The text usually wants you to tap a link or call a number. Once you do, they ask for information or money.

What Scam Texts Look Like

The FTC lists these common tricks:

- Bait: a free prize, gift card or coupon; a credit card with low or no interest; help paying off student loans.
- A false alert: suspicious activity on your account, a payment problem, or an invoice for something you did not buy.
- A fake package delivery notice.

The FTC warns that the link may go to a fake site that looks like the real one. If you sign in there, the scammer gets your username and password. Some links install harmful software on the phone.

What to Do

- Do not tap links in a text you did not expect, especially one that asks for personal or money information.
- The FTC says real companies won't ask for your account information by text.
- If you think the message might be real, contact the company yourself using a phone number or website you already know is real. Do not use the number or link in the text.

How to Report a Scam Text

The FTC gives three ways:

1. Forward the text to 7726 (the letters SPAM). This helps your wireless carrier spot and block similar texts.

2. Use the Report Junk or Report Spam option in your messaging app.
3. Report it to the FTC at ReportFraud.ftc.gov.

After you report it, delete the text.

Filter and Block

The FTC suggests three ways to cut down on scam texts:

- Turn on your phone's filter for unknown senders or spam. Look in the settings for your Messages app, or search Settings for "spam" or "unknown."
- Ask your wireless carrier what call and text blocking it offers. The wireless industry group CTIA lists options at ctia.org.
- Use a call-blocking app.

If You Already Tapped or Answered Do not panic. If you typed a password into a page from a text, change that password right away from the real app or website, and on any other account that uses the same password. If you gave a bank or card number, call the number on the back of your card. For a full recovery plan, see the companion guide Scams and Identity Theft, or go to IdentityTheft.gov.

Checklist

☐ I know to forward scam texts to 7726.

☐ My unknown-sender or spam filter is on.

☐ I never use a link or number from an unexpected text.

Chapter 7: Protect Your Phone Number

Your phone number is the key to many of your accounts. Banks and email services send sign-in codes to it by text. If a criminal takes over your number, those codes go to them.

How a SIM Swap Works

The FTC explains that in a SIM swap, a scammer calls your wireless carrier, claims your phone was lost or damaged, and asks the carrier to move your number to a new SIM card in a phone the scammer has. Once that happens, your phone loses service and the scammer gets your calls and texts, including sign-in codes.

How to Protect Yourself

The FTC recommends:

- Do not reply to calls, emails or texts that ask for personal information. Contact the company yourself using a number or website you know is real.
- Limit the personal information you post online.
- Set a PIN or password on your wireless carrier account. Call your carrier or check its app to set one. Write down that you set it, and keep the PIN somewhere safe.
- If you are worried about SIM swaps, use an authentication app or a security key for important accounts instead of text-message codes.

Warning Signs

If your phone suddenly shows “No Service” or “SOS only” in a place where it normally works, and restarting does not fix it, treat it as urgent. Call your carrier from another phone.

If It Happens to You

The FTC says to:

1. Contact your wireless carrier right away to get your number back, then change your account passwords.
2. Check your credit card, bank and other money accounts for charges or changes you did not make, and report them to the company.
3. If your Social Security, credit card or bank account information was exposed, go to IdentityTheft.gov for a recovery plan.

Checklist

☐ My carrier account has a PIN or password.

☐ My most important accounts use an app or security key, not text codes, where offered.

☐ I know how to reach my carrier from another phone.

Chapter 8: Battery Care

Phone batteries wear out slowly with use. Good habits make yours last longer between charges and longer before it needs replacing.

iPhone

Apple's charging features are on by default:

- iPhone 15 and later: Settings, then Battery, then Charging. You can set a charge limit from 80 to 100 percent in 5 percent steps. Optimized Battery Charging works when the limit is 100 percent.
- iPhone 14 and earlier: Settings, then Battery, then Battery Health and Charging, where you can turn Optimized Battery Charging on or off.

Apple says Optimized Battery Charging delays charging past 80 percent in some situations, so the battery spends less time full. It learns your daily routine over at least 14 days. If you need a full charge now, touch and hold the notice on the Lock Screen and tap Charge Now. Apple warns that turning off these features can increase wear on the battery and shorten its life. Leave them on.

Android

Google's Android Help suggests these ways to get more life from a charge. Exact steps vary by maker.

- Let the screen turn off sooner, lower the brightness, or use auto brightness.
- Turn on dark theme and adaptive battery.
- Use Battery Saver (Settings, then Battery, then Battery Saver), which limits background activity. You can set it to turn on by schedule.

- Turn off Bluetooth and Location when you are not using them, and use Wi-Fi instead of mobile data where you can.
- Restrict apps that use a lot of battery.

Google says the biggest drains include long navigation, video, streaming, games, heavy camera use and using the phone as a hotspot.

Heat Is the Enemy

Google's page says a battery drains much faster when it is hot. In a Northern Nevada summer, a phone left on the dashboard or in a closed car heats up fast. Keep it out of direct sun, and take it out of a thick case if it gets hot while charging.

Chargers

Google says to use the adapter that came with the phone. If you buy a new charger or cable, buy one from the phone maker or a known brand at a real store. Cheap, unbranded chargers are not worth the risk to a phone that costs hundreds of dollars.

When the Battery Is Worn Out If the phone dies by mid-afternoon with normal use, or shuts off with charge still showing, the battery may need replacing. A battery replacement costs far less than a new phone. Use the maker's service or an authorized repair shop.

Checklist

☐ Optimized or adaptive charging is on.

☐ I keep the phone out of hot cars and direct sun.

☐ I use the maker's charger or a known brand.

Chapter 9: If Your Phone Is Lost or Stolen

Move fast. The steps below come from Apple's and Google's own help pages.

iPhone

Apple's page for a stolen iPhone gives these steps:

1. Go to iCloud.com/find on another device. Under All Devices, pick the phone and choose Mark as Lost. This locks it with its passcode.
2. Apple says not to add contact information when it asks, because a thief could use it to trick you.
3. Do not remove the phone from Find My. That would also turn off Activation Lock, which keeps a thief from using it.
4. Even if Stolen Device Protection is on, still mark the phone as lost.
5. If the phone shows somewhere you do not recognize, do not try to get it back yourself. Contact law enforcement.
6. Report the theft to the police. They may ask for the serial number, which Apple says you can find even without the phone.
7. Call your wireless carrier. Ask them to suspend the line and, if your plan covers it, file a claim.
8. If you cannot get the phone back, erase it from Find My or iCloud.com/find. Apple says erasing cannot be undone.
9. Review your Apple Account at account.apple.com: remove devices you do not recognize, check the email addresses,

phone numbers and recovery methods, and change your password if anything looks wrong.

Apple also warns that it will never contact you to say your phone has been found, and to never share your passcode, passwords or verification codes. Texts that say “your lost iPhone has been found” are a common scam.

If Find My was not on before the phone was taken, Apple says you cannot lock or erase it. Change your Apple Account password right away.

Android

Google’s Find Hub page gives these steps:

1. Open the Find Hub app on another device, or go to android.com/find in a web browser, and sign in with your Google Account.
2. Pick the phone. If it is nearby, Play sound rings it at full volume for 5 minutes.
3. Choose Mark as lost to lock it. You can add a message and a contact number for the lock screen.
4. If you cannot get it back, choose Factory reset to erase it. Google warns this permanently deletes the data on the phone.

Google says the phone must have power, be connected to mobile data or Wi-Fi, and be signed in with Find Hub turned on for these steps to work. Then call your carrier to suspend the line and change your Google Account password.

Afterward

- Change passwords on email, banking and any account that was signed in on the phone.

- Watch your bank and card statements for charges you did not make.
- Set up the new phone from your backup.

Checklist

☐ I know my Apple or Google Account password without my phone.

☐ I wrote down my carrier's phone number and my phone's serial number on the page at the back.

Monthly Phone Check

Check	How
System update	iPhone: Settings, General, Software Update. Android: Settings, System, Software updates.
Backup date	iPhone: Settings, your name, iCloud, iCloud Backup. Android: Settings, Google, All services, Backup.
App updates	App Store or Google Play Store
Unused apps	Delete apps you have not opened in months
Location access	Review which apps can see your location
Scam texts	Forward to 7726, then delete
Battery	Charging protection on; phone kept out of hot cars

My Phone Numbers

Keep this page somewhere other than your phone. Do not write passwords here.

Item	Write it here
Phone make and model	_____
Serial number	_____
IMEI (Android: Find Hub, device, Settings)	_____
Apple or Google Account email	_____
Where my account password is kept	_____
Wireless carrier and phone number	_____
Carrier account PIN is set (yes or no)	_____
Insurance or protection plan	_____

Where to Get Help

Who	Where
Find a lost iPhone	iCloud.com/find
Find a lost Android phone	android.com/find or the Find Hub app
Report a scam text	Forward to 7726; ReportFraud.ftc.gov
Identity theft recovery plan	IdentityTheft.gov
Apple Support	support.apple.com
Android Help	support.google.com/android

Acronyms

CTIA. The wireless industry trade group (the letters are its name)

FTC. Federal Trade Commission

GB. Gigabyte, a measure of storage

IMEI. International Mobile Equipment Identity, a phone's unique number

iOS. The iPhone operating system

PIN. Personal identification number

SIM. Subscriber identity module, the card or chip that ties a phone to your number

SMS. Short message service, a standard text message

Sources

All web pages were read on November 18, 2026.

- Federal Trade Commission, How to Recognize and Report Spam Text Messages (consumer.ftc.gov).
- Federal Trade Commission, SIM Swap Scams: How to Protect Yourself, consumer alert, October 23, 2019.
- Apple Support, Update your iPhone or iPad (published October 5, 2026).
- Apple Support, How to back up your iPhone or iPad with iCloud (published September 24, 2026).
- Apple Support, About Charge Limit and Optimized Battery Charging on iPhone (published December 8, 2025).
- Apple Support, About Stolen Device Protection for iPhone (published October 22, 2026).
- Apple Support, About privacy and Location Services in iOS, iPadOS, and watchOS (published May 20, 2026).
- Apple Support, If your iPhone or iPad was stolen (published June 24, 2026).
- Google Android Help, Check and update your Android version.
- Google Android Help, Back up or restore data on your Android device.
- Google Android Help, Find, secure, or erase a lost Android device.
- Google Android Help, Get the most life from your Android device's battery.
- Google Android Help, Change app permissions on your Android phone.
- Google Play Help, Use Google Play Protect to help keep your apps safe and your data private.

About This Book

Keeping Your Phone Safe and Healthy is part of a set of free plain-language guides from Trinfinity Enterprises, and a companion to Keeping Your Windows PC Healthy and Scams and Identity Theft. Menu names and steps were checked against Apple, Google and Federal Trade Commission pages as of November 18, 2026. Phone makers change menus with updates, so if a step looks different on your phone, search Settings for the feature name. This book is general information, not technical support. If you find something that has changed or needs correcting, please write to andrew@trinfinityenterprises.com.