BILL'S HOME TECH

Home & Small Business Tech Solutions

AN EXTENDED GUIDE · NO. 2322

Updated November 2026

Turn On the Scam Protections Built Into Your Phone

Free, hidden settings on iPhone and Android that silence scam calls and filter scam texts

Plain-English tech help from:

Bill's Home Tech

Portage County, Ohio

Tech Made Simple. Service Made Personal.

Bill Davis — Bill's Home Tech

(330) 200-8042 · bill@billshometech.com · Atwater, Ohio

Book a visit · billshometech.com/book

What's Inside

Everything in this guide, with page numbers. Skip to whichever chapter answers your question right now.

The 60-Second Version 3
The Short Version 3
What Your Phone Can and Can't Do 4
iPhone: Screen or Silence Unknown Callers 4
iPhone: Filter Unknown Text Senders 5
iPhone: Keep the Built-In Shields Up 6
Android: Turn On Caller ID & Spam Protection 6
Android: Filter Spam Texts 7
Android: Turn On Extra Protection 7
A Setting Scammers Try to Use Against You 8
Build Good Habits Around the Settings 9
A Yearly Phone Safety Check-Up 9
Set It Up for a Loved One 10
When to Call Bill 10
Everyday Cheat Sheet 12
A Note From Bill 13
Your Visit — and My Promise 14

SUMMARY

The 60-Second Version

Your phone has free scam protections built in that are usually switched off by default. On iPhone, open Settings and the Phone options to screen or silence unknown callers, and turn on Filter Unknown Senders under Messages. On Android, open the Phone app's settings for Caller ID & spam and any Scam Detection, and turn on Spam protection in the Messages app.

On both, keep the phone and apps updating automatically, since many scams rely on old software. These tools thin the flood so fewer attempts reach you, but they're a filter, not a force field — your own judgment still matters. And never install a remote-control app because an unexpected caller asked you to; that hands them your phone.

- iPhone: screen/silence unknown callers; Filter Unknown Senders for texts.
- Android: Caller ID & spam and Scam Detection; Messages spam protection.
- Keep everything updating automatically, and never install a caller's remote-access app.

1 The Short Version

Your phone already has powerful scam protections built right in — you just have to switch them on. These free, hidden settings can silence or screen unknown callers, filter scam texts into a separate list, warn you about suspicious links, and more. Turning them on is a one-time job that quietly cuts down the daily flood of scam calls and texts and catches many that slip through.

This guide walks through the key settings for both iPhone and Android in plain language. Menu names shift a little between phone models and updates, so we'll describe where to look rather than promising exact taps — and if you'd rather, I'm happy to set them all up with you in a single visit.

- Your phone has free scam protections built in; most are just turned off by default.

- Call screening and spam filtering cut down scam calls and texts dramatically.
- These work alongside your good habits — they thin the flood so fewer attempts reach you.
- Setup is a one-time job; we'll cover iPhone and Android both.

> **WATCH OUT**
>
> No setting catches everything, and that's fine. The point is to shrink the number of scam calls and texts that ever reach you, so your attention is saved for the few that do get through — where your own good judgment takes over.

2 What Your Phone Can and Can't Do

It helps to set honest expectations. These tools are genuinely useful, but they're a strong filter, not a force field. Understanding that keeps you from either ignoring them or trusting them blindly.

- They can silence or screen calls from numbers not in your contacts.
- They can sort suspected spam texts into a separate folder.
- They can warn you about some known scam links and dangerous sites.
- They can't read a scammer's mind — a clever live caller can still get through.

> **GOOD TO KNOW**
>
> Think of these settings like a good screen door: they keep out most of the bugs so the house is pleasant, but you still look before you let a stranger in. The settings handle the volume; you handle the judgment.

3 iPhone: Screen or Silence Unknown Callers

Recent iPhone software (iOS 26) added a strong call-screening feature. You choose how your phone handles calls from numbers that aren't in your contacts, and the options range from gentle to strict.

1. Open Settings, then scroll to Apps and open Phone (on some versions, Phone appears directly in Settings).
2. Look for the section about screening unknown callers.
3. Choose the option that fits you: 'Ask Reason for Calling' has the phone ask unknown callers who they are and why, and shows you their answer before you pick up.
4. Or choose 'Silence' to send unknown callers straight to voicemail, where you can review them later.
5. Leave it on 'Never' only if you want no screening at all.

> **WATCH OUT**
> 'Silence Unknown Callers' is very effective against spam, but it also quiets legitimate calls from numbers you haven't saved — a doctor's office, a delivery, a new contact. If you're expecting an important call from a new number, the screening option is often the gentler choice.

4 iPhone: Filter Unknown Text Senders

Your iPhone can tuck texts from people not in your contacts into a separate list, so scam texts don't sit right alongside messages from family.

1. Open Settings and find Messages (via Apps on newer versions).
2. Turn on 'Filter Unknown Senders.'
3. Your Messages app will now show a separate tab for texts from unknown numbers.
4. Glance at that tab now and then for anything real, and ignore the rest.

> **WATCH OUT**
> When a scam text arrives from an unknown sender, you can also tap 'Report Junk' beneath it, which reports and deletes it. And forwarding scam texts to 7726 (which spells SPAM) tells your carrier, too.

5 iPhone: Keep the Built-In Shields Up

A few more iPhone settings quietly protect you, and they're on by default — it's worth confirming they haven't been switched off.

- Keep iOS updated (Settings, General, Software Update) — updates patch security holes scammers exploit.
- Leave the fraudulent-website warning on in Safari's settings for an extra heads-up on scam sites.
- Keep two-factor authentication on for your Apple Account, so your photos, backups, and purchases stay locked to you.
- Use a strong passcode, and Face ID or Touch ID, so a lost phone can't be rummaged through.

> **GOOD TO KNOW**
>
> Keeping the phone updated is one of the most powerful and overlooked protections. Many scams and viruses rely on old, unpatched software; an up-to-date phone simply closes those doors.

6 Android: Turn On Caller ID & Spam Protection

Most Android phones with the Google Phone app can flag or filter suspected spam calls, and newer versions can even detect likely scam calls as they happen.

1. Open the Phone app, tap the three-dot menu, and open Settings.
2. Find 'Caller ID & spam' and turn on both caller ID and spam filtering.
3. If your phone offers 'Filter spam calls,' turning it on sends suspected spam straight to voicemail.
4. Look for a Scam Detection feature, if your phone has it, which listens for scam patterns during a call and warns you.

GOOD TO KNOW

Android's newer Scam Detection works on the device itself to spot the tactics scammers use on a live call and alert you. Google is clear that it isn't perfect, so treat its warning as a strong nudge to hang up and verify, not the only line of defense.

Rather not do this yourself? I'll come to your home and set it up for you — a flat $99 first visit across Portage County, Ohio and nearby communities. Outside the area? I also help remotely by phone or screen-share. Book at billshometech.com/book or call (330) 200-8042.

7 Android: Filter Spam Texts

The Google Messages app can detect and sort likely spam texts, and warn you about dangerous links.

1. Open the Messages app, tap your profile or the three-dot menu, and open Settings.
2. Open 'Spam protection' and make sure it's turned on.
3. Suspected spam will be moved to a Spam folder you can review.
4. Use 'Report spam' on bad texts, and you can also forward scam texts to 7726.

WATCH OUT

Android's Messages also offers scam and link warnings that flag suspicious texts and risky web links. Leaving these on gives you a gentle heads-up right when it matters most — just before you'd tap.

8 Android: Turn On Extra Protection

Android has deeper safety features worth switching on, including a strong anti-fraud setting and, for those who want the highest guard, an advanced protection mode.

- Keep Google Play Protect on (in the Play Store settings) — it scans apps for harmful behavior.
- Keep Android updated (Settings, System, Software/System update) to close security gaps.
- Consider Advanced Protection, which bundles Google's strongest security settings for high-risk users into one switch.
- Only install apps from the official Play Store, and review what permissions an app asks for.

> **WATCH OUT**
> Be very cautious about installing apps from outside the Play Store or from a link someone sends you. 'Sideloaded' apps skip Google's safety checks and are a common way scammers slip harmful software onto a phone.

9 A Setting Scammers Try to Use Against You

One trick deserves special mention: scammers sometimes talk a victim into installing a remote-control or screen-sharing app so they can 'help fix a problem.' This hands them the keys to your phone.

- Never install a remote-access or screen-sharing app because an unexpected caller asked you to.
- No real bank, tech company, or government agency needs to control your phone remotely.
- If you ever did install one at a caller's request, remove it right away.

> **WATCH OUT**
> This is one of the most damaging tricks going, because once a scammer can see and control your screen, they can move money while you watch. If anyone on the phone asks you to install something so they can 'take a look,' hang up — and if it already happened, call me so we can clean it up.

10 Build Good Habits Around the Settings

The settings do the heavy lifting on volume, but a few simple habits make them far stronger. Together they form a calm, confident way of using your phone.

- Let unknown calls go to voicemail; if it's real, they'll leave a message and you can call back.
- Don't tap links in unexpected texts, even ones that slipped past the filter.
- Add the people you care about to your contacts so their calls always ring through.
- Keep the phone updated — turn on automatic updates so you don't have to remember.

> **TIP**
>
> Turning on automatic updates (for both your phone's software and your apps) means your protections quietly stay current without you lifting a finger. It's the easiest safety habit there is.

11 A Yearly Phone Safety Check-Up

Settings can drift over time — an update resets something, or you turn a filter off to catch one call and forget to turn it back on. A quick yearly look keeps your protections sharp.

1. Confirm call screening or silencing is still on and set the way you like.
2. Check that text spam filtering is still turned on in your messaging app.
3. Make sure automatic updates for the phone and apps are still enabled.
4. Review the apps on your phone and remove any you don't recognize or no longer use.
5. Glance at which apps have permission to your microphone, camera, and location, and trim anything odd.

GOOD TO KNOW

Reviewing app permissions now and then is quietly powerful. Apps sometimes ask for far more access than they need, and trimming that back shrinks how much of your life any single app — or a sneaky one — can reach.

12 Set It Up for a Loved One

These settings are a wonderful gift to set up for a parent or friend who gets too many scam calls. A calmer phone is a safer phone.

1. Turn on call screening or silencing so the constant spam calls stop.
2. Switch on text spam filtering so scam texts don't crowd their inbox.
3. Make sure family and key contacts are saved so those calls always come through.
4. Turn on automatic updates so protections stay current without any effort.

GOOD TO KNOW

For someone overwhelmed by scam calls, simply turning on call silencing or screening can transform their day. Fewer frightening calls means less anxiety and far fewer chances to be caught off guard.

13 When to Call Bill

Every setting here is something you can switch on yourself, and this guide gets you there. But menu names move around between phones and updates, and if you'd rather have it all done right in one sitting — yours or a loved one's — that's a quick, satisfying visit.

I'll turn on call screening and spam filtering, set up text and link warnings, confirm your phone and apps update automatically, make sure the people you care about always ring through, and remove any remote-control app that shouldn't be there. You'll leave with a quieter, safer phone and a clear sense of what each setting does.

- You want all the scam protections turned on properly in one go.
- You're setting up a phone for a parent who gets too many scam calls.
- You're not sure which screening option is right for your life.
- You may have installed something at a caller's request and want it checked.

CHEAT SHEET

Everyday Cheat Sheet

Keep this handy. Turn these on once and enjoy a quieter, safer phone.

I want to...	Do this...
Stop spam calls (iPhone)	Settings > Phone > screen or silence unknown callers
Stop spam texts (iPhone)	Settings > Messages > Filter Unknown Senders
Stop spam calls (Android)	Phone app > Settings > Caller ID & spam (and Scam Detection)
Stop spam texts (Android)	Messages > Settings > Spam protection on
Stay patched	Turn on automatic updates for your phone and apps
Avoid the worst trap	Never install a remote-control app a caller asks for
Get help	Call Bill: (330) 200-8042

BEFORE YOU GO

A Note From Bill

A quick note from Bill. I write these guides to make home tech a little less frustrating, and I do my best to keep every step accurate and up to date. Still, every home, device, and setup is a bit different, so I can't promise a guide will match yours exactly or fix your particular problem. These guides are for general information only — they're not professional, legal, or financial advice, and they don't replace your device's own manual or the manufacturer's instructions. Please go slow, use your own good judgment, and use everything here at your own risk. If a step involves electrical wiring, a gas appliance, a water heater, plumbing, or climbing a ladder — or if anything just doesn't feel safe — please stop and call a licensed professional (or give me a call at 330-200-8042). Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results.

HOW I CAN HELP

Your Visit — and My Promise

You don't have to remember all of it — just that a friendly, patient person is one call away, whenever you'd rather have a hand.

KEY SPECS

In your home — $99 flat for the first visit, no contracts and no surprises, with a 30-day come-back-free follow-up. In-home visits cover Portage County, Ohio and nearby communities.
Outside the area? Remotely — $49 for a screen-share session (free for Support Plan members, $39/mo), refundable if I can't fix it — and credited toward a visit if you'd rather have me in person. Book either at billshometech.com/book.

GOOD TO KNOW

My promise — If you're not 100% satisfied with your visit, I'll come back at no charge, or refund the full $99. No questions, no awkwardness. That's how I'd want to be treated.

Whenever you're ready, I'll come to your home anywhere in Portage County, Ohio and nearby communities, at your pace. Too far for a house call? I also help remotely. Book at billshometech.com/book or call (330) 200-8042. — Bill

Call or text (330) 200-8042 · bill@billshometech.com

This free guide is for general information only — not professional advice, and no substitute for your device's own manual. Any prices or outside products mentioned can change; please confirm current details before you buy. Please use your own good judgment and follow it at your own risk — for anything involving electricity, gas, water, or heights, stop and call a licensed professional. Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results. © 2026 Bill's Home Tech, LLC.