BILL'S HOME TECH

Home & Small Business Tech Solutions

AN EXTENDED GUIDE · NO. 2344

Updated November 2026

Lock Settings During Calls (Scam Defense)

Shut the door on the "stay on the line" scam — and the one habit that defeats it

Plain-English Android 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

How the "Stay on the Line" Scam Works 4

The One Habit That Beats It Every Time 4

Lock Down Installing Unknown Apps 5

Block Screen-Sharing and Remote-Control Apps 6

Protect the Settings Themselves 6

Guard Your Verification Codes 7

Set Up Call Screening and Scam Filtering 8

What to Do If You're On a Suspicious Call Right Now 8

If You Think You Already Acted 9

The Scams Worth Knowing by Name 9

Teaching the Habit to Someone You Care For 10

When to Call Bill 11

Everyday Cheat Sheet 12

A Note From Bill 13

Your Visit — and My Promise 14

SUMMARY

The 60-Second Version

The "stay on the line" scam depends on a stranger directing your phone while you listen. The one habit that defeats it: nobody legitimate — not your bank, not Microsoft, not a government office — calls you out of the blue and walks you through installing an app, changing a setting, or reading out a code.

The moment a caller does that, hang up, and call the company back on the number from your own card. As a safety net, keep "Install unknown apps" turned off, never install a screen-share app for a caller, never read a code aloud, and turn on your Phone app's spam filtering and "Silence unknown callers."

If you think you already acted, call Bill right away — no judgment.

1 The Short Version

One of the nastiest scams aimed at older adults works like this: a stranger calls, claims to be from your bank, Microsoft, Amazon, or a government office, and — while keeping you on the phone — talks you through changing settings, installing an app, or reading out a code. The whole trick depends on getting you to do things on your phone while they stay in your ear. This guide is about making that far harder, and about the one habit that defeats it entirely.

You can set your phone up so that the moves a scammer needs — installing unknown apps, screen-sharing, changing key settings — are blocked or locked behind your fingerprint or PIN. Combined with the golden rule of never acting on an out-of-the-blue call, these settings close the door on this kind of fraud.

- This scam depends on you doing things on your phone while a stranger directs you.
- You can lock down the exact moves they need, so the scam can't get going.
- The golden rule: anyone who contacts you out of the blue and creates urgency is a scammer.

- None of these settings get in your way in normal everyday use.

> **WATCH OUT**
> Write this on a card by your phone: "No real company or agency will ever call me and walk me through my phone settings. If they do, it's a scam — hang up." That one sentence prevents nearly all of this.

2 How the "Stay on the Line" Scam Works

Understanding the shape of the scam makes it easy to spot. It almost always follows the same script, because the script works on people when they're caught off guard.

- A call or message arrives out of the blue, claiming a problem: fraud on your account, a virus, a refund owed, a package issue.
- It creates urgency and fear — act now, or lose your money, or be arrested.
- They insist you stay on the phone and not hang up or call anyone.
- They direct you to install an app, change a setting, or read a code aloud.
- That app or setting hands them control, or the code lets them in.

> **GOOD TO KNOW**
> The pressure to "stay on the line" is itself the biggest red flag. They do it precisely so you can't pause, hang up, and call the real company — which would end the scam instantly. Recognizing that pressure as the tell is half the battle.

3 The One Habit That Beats It Every Time

Before any settings, know this: the settings in this guide are a safety net, but the real defense is a habit, and it's simple enough to never forget.

> *Nobody legitimate calls you out of the blue and walks you through your phone. If they do, it's a scam — hang up.*

Your bank, Microsoft, Apple, Google, Amazon, the IRS, Medicare, the Social Security office — none of them will ever call you unexpectedly and direct you to install something, change a setting, or read out a code. Not one. So the moment a caller starts doing that, you already have your answer. Hang up, and if you're worried it might be real, call the company back on the number printed on your card or statement — never a number the caller gives you.

WATCH OUT

Scammers can make any name or number show up on your screen — your bank's name, even a local number. So "but it said it was my bank" is not proof. The caller ID can be faked completely. Judge the call by what they ask you to do, not by what the screen says.

4 Lock Down Installing Unknown Apps

A favorite scammer move is to have you install a "support" or "security" app that actually lets them see and control your screen. Android already blocks apps from outside the official Play Store by default, but it's worth confirming that guard is firmly in place.

1. Open Settings and search for "Install unknown apps" or "Special app access."
2. Open the list of apps allowed to install others — ideally it should be empty or all turned off.
3. Turn off permission for your browser and any messaging apps to install unknown apps.
4. This means apps can only come from the official Play Store, which is exactly what you want.

GOOD TO KNOW

Turning on Advanced Protection (covered in its own guide) locks this down automatically and keeps it locked. If you've done that, this is already handled — but confirming it here does no harm.

5 Block Screen-Sharing and Remote-Control Apps

The apps scammers most want you to install are "remote access" or "screen-share" tools — ones with names like AnyDesk, TeamViewer, or anything offering "remote support." In the right hands these are legitimate; in a scam, they hand a stranger your screen and your taps. The defense is simple: never install one at a stranger's request.

WATCH OUT

If a caller asks you to install any app so they can "see your screen" or "fix it remotely," that is a scam, every time, no exceptions. Hang up. A real technician you called yourself might use such a tool — but only one you contacted first, never one that contacted you.

1. If you ever installed such an app at someone's urging, remove it now: long-press its icon Uninstall.
2. Check Settings Accessibility and turn off anything you don't recognize — scam apps hide here to watch your screen.
3. If you're unsure what's safe to remove, leave it and call Bill rather than guess.

6 Protect the Settings Themselves

You can add friction to the settings a scammer would need to change, so that even a moment of pressure doesn't let something slip through. The aim is to make the risky moves require your fingerprint, face, or PIN.

- Keep a screen lock on — a PIN, pattern, or fingerprint — so the phone can't be changed while it sits unlocked.
- Set the screen to lock quickly when idle, so a handed-over phone re-locks on its own.
- Where your phone allows it, require your fingerprint or PIN to change security settings.
- Turn on Advanced Protection, which locks several of these in place at once.

GOOD TO KNOW

Some phones and some apps let you "pin" a single app to the screen, so nothing else can be opened without your PIN. It's handy if you ever hand your unlocked phone to someone to show them one thing — they can't wander into your settings or accounts.

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 Guard Your Verification Codes

Those six-digit codes that arrive by text to confirm it's really you are a favorite scammer target. If they can get you to read one aloud, they can get into your account. The rule about codes is as firm as the rule about calls.

WATCH OUT

Never read a verification or security code aloud to anyone, and never type one into a website someone sent you. Real companies send those codes TO you to type into THEIR app yourself — they never phone to ask you to say one back. Anyone asking for your code is trying to break into your account.

WATCH OUT

The text messages carrying these codes usually say, in the message itself, "never share this code with anyone." That warning is there for exactly this reason. Take it literally — even if the caller sounds official and urgent.

8 Set Up Call Screening and Scam Filtering

Your phone can take a lot of these calls before they ever reach you. Turning on the Phone app's built-in protections means many scam and spam calls are flagged, silenced, or screened automatically.

1. Open the Phone app, tap the three dots or your profile, and open Settings.
2. Turn on "Caller ID & spam" so suspected spam calls are labeled.
3. Turn on "Scam Detection" if your phone offers it, for mid-call warnings.
4. Consider "Silence unknown callers," which sends calls from numbers not in your contacts to voicemail.

GOOD TO KNOW

"Silence unknown callers" is a powerful setting for peace of mind. Real callers who need you — a doctor's office, say — will leave a voicemail, and you can call them back. It cuts out the cold scam calls entirely without you lifting a finger.

9 What to Do If You're On a Suspicious Call Right Now

If you're reading this because a call feels wrong as it's happening, here's exactly what to do. You don't owe the caller anything, including politeness.

1. Stop doing whatever they asked. Don't tap, install, or read anything out.
2. Hang up. You're allowed to hang up on anyone, mid-sentence, for any reason.
3. Don't call back the number they called from.

4. If it claimed to be your bank or a company, call them on the number from your card or statement.
5. Tell someone you trust what happened — a second opinion breaks the spell.

> **WATCH OUT**
> If you think you may have already tapped something, installed an app, or shared a code, don't panic — but do call me right away. The sooner we remove a bad app, change passwords, and check your accounts, the better. I've helped many people through exactly this, with no judgment.

10 If You Think You Already Acted

If a call got further than you'd like before you realized, acting quickly limits the damage. Most of this is recoverable, especially if you move fast.

- Remove any app they had you install (long-press Uninstall), and turn off anything odd in Accessibility.
- Call your bank — on their official number — if money or account details were involved.
- Change the password on any account whose code or details you shared.
- Turn the phone off and on, and have someone you trust check it over.
- Report it: you did nothing shameful, and reporting helps stop them targeting others.

> **GOOD TO KNOW**
> Scammers are professionals who fool careful, intelligent people every day. Being caught off guard is not a failure of yours — it's their whole job. What matters is acting now, and there's no shame in calling for help.

11 The Scams Worth Knowing by Name

Scammers reuse a small number of scripts, and recognizing them by name takes away their power. If a call or message matches one of these, you already know it's a fraud.

- The "bank fraud" call: "We've spotted fraud — move your money to a safe account." Your bank never asks this.
- The "grandchild in trouble" call: a panicked voice needing money fast, swearing you to secrecy.
- The "your computer is infected" call or pop-up, urging you to install help or call a number.
- The "refund" or "overpayment" scam: they "accidentally" refund too much and want some back.
- The "package" or "toll" text with a link, asking for a small fee or your details.

GOOD TO KNOW

They all share the same DNA: out of the blue, urgent, and pushing you to act on your phone or with your money right now. Spot that pattern and the specific story doesn't matter — the answer is always to stop and check.

12 Teaching the Habit to Someone You Care For

If you're reading this for a parent, spouse, or friend, the settings matter less than the one habit. Here's how to pass it on in a way that sticks and doesn't feel like a lecture.

1. Share the single sentence: "No real company calls out of the blue and walks you through your phone."
2. Agree on a plan: if a call feels off, they hang up and call you first — always.
3. Write the trusted numbers (bank, you) on a card by the phone, so they never use a number a caller gives.
4. Turn on scam filtering and "Silence unknown callers" together.
5. Reassure them that hanging up on a scammer is never rude, and being targeted is never their fault.

WATCH OUT

The kindest thing you can set up is a simple agreement: "When in doubt, hang up and call me." I'm glad to be a second line in that plan — if a call rattles you or someone you care for, call me and we'll sort out together whether it's real. No judgment, ever.

13 When to Call Bill

Setting these protections up is worthwhile, and this guide walks you through it. But many people would rather have it all done in one careful sitting — the right settings locked in, scam filtering on, and a plain explanation of the one habit that matters most. That's exactly what I'm here for.

I make house calls across Portage County. I'll lock down the moves scammers need, turn on your phone's call and scam protections, check that nothing untoward is already installed, and leave you with a simple card and real confidence. And if a call ever rattles you, I'm a phone call away — no judgment, ever.

- You want all these protections set up properly in one visit.
- A call, text, or pop-up worried you and you want your phone checked.
- You think you may have installed something or shared a code.
- You'd like "Silence unknown callers" and scam filtering turned on.
- You simply want to feel confident you can't be talked into trouble.

CHEAT SHEET

Everyday Cheat Sheet

Keep this by the phone. The habit matters most; the settings are the safety net.

I want to...	Do this...
Beat the scam cold	Nobody real calls out of the blue and walks you through your phone — hang up
Block sneaky installs	Settings "Install unknown apps" turn off for browser and messaging
Refuse remote control	Never install a "screen-share" app for a caller; check Accessibility for odd apps
Protect your codes	Never read a verification code aloud; real companies never phone to ask
Filter scam calls	Phone app Settings Caller ID & spam on; try "Silence unknown callers"
If a call feels wrong	Stop, hang up, call the company on the number from your card
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.