



Caller-ID Spoofing — When "Your Bank," Medicare, or the Sheriff Shows on Your Screen

Why the name on your screen can't be trusted — and the habit that keeps you safe anyway.

————— **An Extended Guide · No. 1626 · SAFETY** —————

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 4
- 1. Why I Wrote This One 4
- 2. What Caller-ID Spoofing Is 5
- 3. Why the Phone Companies Haven't Fixed It 6
- 4. The One Habit That Beats It 7
- 5. The Bank 'Fraud Alert' Disguise 8
- 6. The Government Disguises 9
- 7. The Sheriff and Police Disguise 10
- 8. The 'Neighbor' and Local-Number Trick 10
- 9. When It's Your Own Number Being Faked 11
- 10. The Code They Try to Get 12
- 11. Why This Trick Is So Effective 13
- 12. Tools That Reduce the Flood 14
- 13. A Word on Spoofed Texts, Too 15
- 14. Helping a Loved One With This 15
- 15. When the Faked Voice Joins the Faked Number 16
- 16. A Note on Scary Voicemails 17
- 17. If You Already Shared Something 18
- 18. Questions People Ask Me 18
- 19. A Five-Minute Phone Safety Setup 19
- 20. Reporting It — and Why It Helps 19

21. When to Just Call Me 20

22. Contact Card & a Warm Close 21

Everyday Cheat Sheet 21

A Picture to Follow Along 23

A Second Look 24

A Note From Bill 24

Your Visit — and My Promise 25

SUMMARY

The 60-Second Version

Caller ID can be faked. The name and number on your screen are just a label the caller's system sends along, and scammers can set it to show your bank, Medicare, the IRS, or the local sheriff. So you never trust an incoming call's screen as proof of who is calling. If a call pressures you for money, personal information, or a code, you hang up and call the organization back on a number you look up yourself — from your card, your statement, or their official website — never a number the caller gave you.

- 1 A call shows a trusted name or number — bank, Medicare, sheriff, a local number.
- 2 It pressures you for money, information, or a verification code.
- 3 Remember: the screen is a label, not proof. It can be faked.
- 4 Hang up. Don't use any number the caller gives you.
- 5 Call back on a number you look up yourself, and confirm there.

WATCH OUT

Even a correct, official number on your screen is not proof. Scammers copy real numbers on purpose. The only safe number is one you looked up and dialed yourself.

1. Why I Wrote This One

Because that trusted name on your screen can lie.

In more than thirty years of helping folks across Portage County with their phones and computers, I have watched one quiet assumption get more and more people into trouble: the belief that the name and number on the screen tell you who is really calling. It feels obvious that they would. The phone says 'Huntington Bank' or 'Portage County Sheriff' or shows a local number, so surely it is them. I am writing this guide because that assumption is simply not safe anymore, and letting go of it is one of the most protective things you can do.

The trick is called spoofing, and it lets a scammer make your phone display almost any name or number they choose. They use it to borrow the trust you have in your bank, your doctor, a government agency, or local law enforcement, so that you lower your guard before they have said a word. When the screen shows someone you trust, you are already half-persuaded, which is exactly what the scammer wants.

Here is the reassuring part, as always. You do not need to become a telephone engineer or learn to detect a fake number. You need one simple habit built on one simple truth: the screen is a label, not proof. Once you treat every incoming call's display with friendly skepticism and verify important calls by dialing out yourself, no spoofed number can hurt you. We will walk through how spoofing works, the disguises it wears, and that one habit, step by step and with no rush.

TIP

Share this one with the whole household. The 'trust the screen' habit is deeply ingrained in all of us, and unlearning it together makes it stick.

2. What Caller-ID Spoofing Is

The plain-English version of the trick.

Caller-ID spoofing simply means faking the information your phone shows about who is calling. When a call comes in, the caller's phone system sends along a number, and sometimes a name, that your phone then displays. Crucially, that information is supplied by the caller's side, not verified by some central authority. So a scammer can set it to whatever they like — a real bank's number, a government office, a neighbor's number, anything at all.

It helps to picture it like the return address on an envelope. Anyone can write any return address on a letter they mail; the post office does not check that you really live there. Caller ID works much the same way. The number on your screen is the 'return address' the caller chose to write, and for a long time nothing stopped them from writing a false one. That is why a call can look like it comes from somewhere it absolutely does not.

Scammers use cheap, widely available tools to do this at a massive scale, sending out floods of calls that each wear a trusted disguise. Sometimes they copy a specific real number — your actual bank's published line — so that if you look it up, it matches, making the fake even more convincing. The technology is not exotic or hard for them to get, which is exactly why this has become so common, and why the old instinct to trust the screen now works against you.

GOOD TO KNOW

Think of caller ID like the return address on an envelope: the sender writes it, and no one checks it. A false one is as easy to send as a true one.

3. Why the Phone Companies Haven't Fixed It

The honest state of the defenses.

People reasonably ask why the phone companies cannot just stop this. The answer is that they are working on it, but the fix is partial. The industry and federal regulators have rolled out a system of caller-authentication technology — you may have seen a 'verified' checkmark on some calls — meant to confirm that a call really comes from the number it claims. It genuinely helps with some calls, and it is a step in the right direction, but it is far from a complete cure.

There are several reasons it does not fully solve the problem. The system does not cover every call or every network, especially older landline and some international routes, so many calls still slip through unverified. And even when a call is authenticated, that only confirms it truly came from a particular number — it does not confirm that the person behind the number is honest. A scammer calling from their own verified number is still a scammer.

So the practical takeaway is simple and a little sobering: do not count on the phone network to tell you which calls are safe. The protections are improving, and that is good, but they are nowhere near a guarantee, and they likely never will be a complete one. Your safety cannot rest on technology catching every fake. It has to rest on a habit of your own that works regardless of what the network did or did not verify.

WATCH OUT

A 'verified' or checkmark label on a call is mildly reassuring at best. It does not mean the caller is honest, and most calls do not carry it. Never treat it as a green light.

4. The One Habit That Beats It

Hang up and dial out yourself.

Here is the whole defense in one sentence: for any call that matters — money, personal information, account security, anything official — you hang up and call the organization back on a number you look up yourself. That is it. You do not trust the screen, and you do not use any number or link the caller provides. You end the call and reach the real organization through a channel you control.

This works for the same reason the family callback works against voice cloning: the scammer controls the call that reached you, but they do not control the number you choose to dial. When you hang up and call your bank on the number printed on the back of your card, or the sheriff's office on the number from the county's official website, you leave the scammer's world entirely. A real issue will be waiting for you there; a fake one simply will not exist. The spoofed display becomes irrelevant.

The one critical detail is where you get the number to call back. It must come from somewhere you trust independently — the back of your card, a recent statement, the official website you navigated to yourself, a number you already had saved. Never call back on a number the caller recited, texted, or left in a voicemail, because that just connects you right back to the scammer or an accomplice. The habit is: hang up, find the real number yourself, and call that.

GOOD TO KNOW

Keep your bank's real number (from your card) and a few other key numbers written down by the phone. Having the real number handy makes it easy to hang up and call back the safe way.

5. The Bank 'Fraud Alert' Disguise

One of the most common and convincing.

The most common spoofing disguise is your own bank. Your phone shows the bank's name or its real number, and a calm, professional voice says they have detected fraud or a suspicious charge on your account. They sound exactly like the helpful fraud department you would hope to hear from. Then, to 'protect' you, they ask you to confirm information, read back a code they are sending, or move your money to a 'safe' or 'secure' account while they investigate.

Every one of those requests is the scam. A real bank investigating fraud does not need you to read back the one-time code they texted you — that code is a key, and handing it over unlocks your account for them. A real bank will never ask you to move your money to another account to keep it safe; that instruction exists only to steal it. And a real bank already knows your account details, so it does not need you to confirm your full card number or password over a call you did not place.

So when 'the bank' calls about fraud, however real the screen looks, you thank them, hang up, and call the bank yourself on the number from your card. If the fraud alert was genuine, the real bank will know all about it when you call in, and you can sort it out safely. If it was a scam, you have calmly stepped around it. This single move defeats the most common and costly spoofing scam there is.

WATCH OUT

No real bank ever asks you to read back a code or move your money to a 'safe account.' Those two requests are proof of a scam, no matter what your screen says. Hang up and call the number on your card.

6. The Government Disguises

IRS, Social Security, Medicare, and more.

Scammers love to wear government costumes, because authority makes people anxious and compliant. Your screen might show the IRS, the Social Security Administration, Medicare, or a federal agency, and the caller claims there is a serious problem: back taxes owed, your Social Security number suspended or linked to a crime, your Medicare benefits at risk. The tone is official and often threatening, with hints of arrest, lawsuits, or lost benefits if you do not act at once.

A few plain truths dissolve these. Government agencies generally contact you first by mail, not by surprise threatening phone calls. The IRS does not demand immediate payment by gift cards, wire, or cryptocurrency, and does not threaten to send police over the phone. Your Social Security number cannot be 'suspended,' and the Social Security Administration's own watchdog has long warned that its real numbers are spoofed by scammers — its staff do not call to threaten you or demand payment or personal information to fix a problem.

So treat any threatening 'government' call the same way, regardless of how official the screen and the voice are. You hang up, and if you are genuinely concerned there might be a real issue, you contact the agency through its official website or a number you look up yourself — never a number or link the caller provided. Real agencies will have proper records and will not punish you for verifying. The threats and the demand to act immediately are the surest signs the call is a fraud.

WATCH OUT

Government agencies don't call out of the blue to threaten arrest or demand gift cards, wires, or crypto. A threatening 'IRS' or 'Social Security' call is a scam, even when the screen shows the real agency.

7. The Sheriff and Police Disguise

When the law seems to be on the line.

A particularly intimidating version shows your local sheriff's office or police department on the screen. The caller, often giving a real-sounding name and badge number, says you missed jury duty, have a warrant, or are connected to a crime, and that you can avoid arrest by paying a 'fine' or 'bond' immediately. Because the number may match the real sheriff's office you could look up, and because fear of the law runs deep, this one rattles even sensible people.

The plain truth: real law enforcement does not call to collect money over the phone, and does not take payment in gift cards, wire transfers, or cryptocurrency to clear a warrant. Courts handle missed jury duty through mailed notices and proper legal process, not threatening phone calls demanding instant payment. No legitimate officer will tell you that you can make an arrest warrant disappear by buying store cards and reading off the numbers. The entire premise is false.

So if 'the sheriff' calls demanding money, you can be confident it is a scam, spoofed number and all. Hang up. If the fear lingers and you want to be certain, look up your local sheriff's office number yourself — from the county's official website, not from the call — and ask them directly; they will tell you no such thing is happening. Verifying through a number you found yourself is the move that defeats this disguise as surely as all the others.

WATCH OUT

Police and courts never take gift cards, wires, or crypto to clear a warrant or a missed jury summons. A caller claiming otherwise is a scammer wearing the sheriff's number.

8. The 'Neighbor' and Local-Number Trick

Why so many spam calls look local.

You have probably noticed that many unwanted calls come from numbers that look local — the same area code as yours, sometimes even the same first few digits as your own number. This is a deliberate spoofing tactic sometimes called 'neighbor spoofing.' Scammers and aggressive telemarketers fake a local-looking number because we are far more likely to answer a call that seems to come from someone nearby than one from a distant or unfamiliar area.

It is worth knowing this for two reasons. First, it explains why a local number on your screen is no guarantee the caller is actually local or someone you know; it may just be chosen to get you to pick up. Second, it means that if you answer and the call turns out to be a robocall or a sales pitch or a scam, you have done nothing wrong — you simply fell for a number designed to look familiar. The best response is usually to hang up without engaging.

Some people choose not to answer calls from numbers they do not recognize at all, letting them go to voicemail, which is a perfectly reasonable habit. Legitimate callers will usually leave a message, and you can call back if needed on a verified number. Whether you answer or not, the underlying rule holds: a familiar-looking local number proves nothing about who is really calling, so treat any request for money or information with the same hang-up-and-verify caution.

WATCH OUT

A local-looking number is often just bait to get you to answer. If you don't recognize a number, it is perfectly fine to let it go to voicemail and call back only if it is someone real.

9. When It's Your Own Number Being Faked

If strangers say you called them.

Here is an unsettling twist that catches people off guard: sometimes it is your number that scammers are spoofing, and you find out when strangers start calling or texting you, annoyed, saying you called them when you did not. This happens because the scammer picked your number, at random or from a list, as the fake return address on their mass of scam calls. It feels violating, but it is important to understand what it does and does not mean.

It does not mean your phone has been hacked or that someone has access to your account. The scammers are not calling from your phone; they are simply displaying your number on other people's screens, the same way anyone can write your address on an envelope they mail. There is usually nothing technically wrong with your device, and the activity will typically fade on its own after a while, once the scammers rotate to spoofing a different number.

There is not a great deal you can do to stop it directly, which is frustrating but not dangerous to you. You can let the puzzled callers know, kindly, that your number was spoofed and you did not call them. You can record a brief voicemail greeting noting the same if the calls are heavy. And you can report it to the Federal Communications Commission. Mostly, it is a nuisance that passes. Knowing what it is keeps you from panicking or falling for a follow-up 'we can fix your spoofed number for a fee' scam, which is itself a fraud.

GOOD TO KNOW

If your number is being spoofed, your phone isn't hacked — scammers are just borrowing your number as a disguise. It usually passes. Never pay anyone who offers to 'fix' it.

10. The Code They Try to Get

One-time codes are a favorite target.

Across many of these spoofed calls runs a single, specific goal worth isolating: getting you to read back a one-time verification code. These are the six-digit numbers that a bank, email provider, or other service texts you to confirm it is really you logging in. Many accounts now use them as a second lock beyond your password. A scammer who already has your password only needs that code to get in, and a spoofed 'security' call is how they try to pry it out of you.

The call is clever. 'We're seeing suspicious activity and we're sending a code to verify your identity — can you read it back to confirm it's really you?' In the moment, reading back a number you just received feels harmless, even cooperative. It is the opposite. That code is the key to your account, and the person asking for it is trying to walk through your door. The real service sent the code for you to type in yourself, never to recite to a caller.

So make this an absolute, unbreakable rule: you never give a verification code to anyone who contacts you, for any reason, no matter how official they sound or what your screen shows. No legitimate company will ever ask you to read one back. If a caller wants that code, the request itself proves they are a scammer, and the correct response is to hang up immediately. Guard your codes as fiercely as you would the keys to your house, because that is exactly what they are.

WATCH OUT

'Read me the code we just sent to verify it's you' is always a scam. The code is a lock to keep others out — reading it aloud hands them the key.

11. Why This Trick Is So Effective

Understanding it keeps you humble and safe.

It is worth pausing on why spoofing fools so many careful people, because understanding it protects you better than simply being told to watch out. We have spent our whole lives learning to trust caller ID. For decades, the number on the screen was a reasonable guide to who was calling, and that trust became automatic, the way we trust a familiar voice or a familiar return address. Scammers exploit exactly that deep, reasonable habit.

On top of that, the disguises they choose are the ones most likely to make us act without thinking: our bank, the government, the police. These are authorities we are conditioned to take seriously and to obey quickly, especially when they say something is wrong. Add a dash of manufactured urgency and fear, and a person's careful judgment can be swept aside in seconds. None of that reflects poorly on you; it reflects how well the trick is aimed at normal human instincts.

Recognizing all this does two good things. It removes any shame if you have been fooled or nearly fooled — you were trusting a signal that used to be trustworthy. And it motivates the one change that matters: consciously demoting caller ID in your mind from 'proof' to 'mere suggestion.' Once you have genuinely let go of the belief that the screen tells the truth, the whole family of spoofing scams loses its grip on you, because you are no longer giving the display the trust it no longer deserves.

GOOD TO KNOW

Being fooled by a spoofed number is not a sign of carelessness — it is a sign you trusted a signal that used to be reliable. The fix is to retrain that trust, not to blame yourself.

12. Tools That Reduce the Flood

Cutting down the calls in the first place.

While no tool can make caller ID trustworthy, several can reduce how many spoofed and spam calls reach you, which lowers your exposure and your stress. These are worth setting up, as long as you remember they are a filter, not a guarantee — some scam calls will still get through, and the hang-up-and-verify habit still rules. Think of these as reducing the flood, not replacing the dam.

- Turn on your phone carrier's spam-call filtering or blocking app, which many offer free and which labels or blocks likely scam calls.
- Use your phone's built-in option to silence calls from unknown numbers, sending them to voicemail so real callers can still leave a message.
- Block individual numbers that repeatedly bother you, though scammers do change numbers often.
- Register your number with the national Do Not Call list, which reduces legitimate telemarketing, even if it does not stop scammers.
- Report persistent scam and spoofed calls to the Federal Communications Commission.

The option to silence unknown callers is especially helpful for many older adults. Calls from people in your contacts still ring through normally, while unknown numbers go quietly to voicemail, where you can review them at your leisure and call back only the real ones on verified numbers. It can feel like a wonderful relief after a stretch of relentless spam, and it dramatically cuts the chances of being caught off guard by a spoofed call in the first place.

GOOD TO KNOW

If spam calls are wearing you down, ask me about turning on 'silence unknown callers' and your carrier's free spam filter. Together they can quiet the phone dramatically while still letting real callers reach you.

13. A Word on Spoofed Texts, Too

The screen lies in messages as well.

Spoofing is not limited to phone calls. The same kind of faking happens with text messages, where a scam text can appear to come from your bank, a delivery company, a toll agency, or even a name rather than a number, so it slots neatly into an existing thread of real messages. A fake fraud alert or 'package held' text that lands right under genuine messages from the same sender is especially convincing, because the phone groups them together as if they are all from one place.

The habit transfers exactly. A text asking you to tap a link, call a number, confirm details, or pay a fee gets the same treatment as a call: you do not act through the message. You reach the company yourself through its app, your saved bookmark, or the number on your card, and confirm there. The fact that a scam text appears in the same thread as real ones does not make it real — it just means the sender name or number was faked to match.

Two quick extras for texts. You can report scam texts by forwarding them to 7726, which spells SPAM, helping your carrier block the source. And resist the urge to reply, even to say 'stop' or to tell them they have the wrong person — with a scammer, any reply simply confirms your number is active and worth targeting more. Just delete it, verify independently if it claimed to be someone you deal with, and move on.

WATCH OUT

A scam text can land right inside a real message thread by faking the sender. Appearing alongside genuine texts does not make it genuine — verify through the company's own app, not the message.

14. Helping a Loved One With This

Unlearning 'trust the screen' together.

The belief that caller ID is trustworthy is so deep and so widely shared that helping a loved one let go of it takes patience and repetition rather than a single conversation. If an older parent or a less tech-comfortable spouse keeps trusting the screen, do not scold or make them feel foolish; the belief was reasonable for most of their life. Instead, gently and repeatedly reinforce the one simple idea: the screen is a label anyone can print, so we always call back on a number we look up ourselves.

Make it concrete and easy to act on. Help them write their bank's real number, from the card, on a note by the phone, along with a short reminder: 'Bank called? Hang up and call this number.' Set up their phone's spam filtering and, if they would like it, the silence-unknown-callers option. Practice the hang-up-and-call-back routine together once or twice so it feels familiar. The goal is to make the safe response the automatic one, so it holds even when a scary 'official' call comes.

Above all, make sure they know they can always call you, or someone they trust, before acting on any worrying call, with no judgment at all. Scammers count on isolating people, so simply being the calm person your loved one checks with breaks the whole scheme. Reassure them, often, that no real bank, agency, or officer will ever mind them hanging up to verify — and that you will never think less of them for asking.

TIP

Write 'Hang up and call this number' plus the bank's real number on a card by the phone. A visible reminder beats memory when a convincing official call lands.

15. When the Faked Voice Joins the Faked Number

Spoofing plus AI makes a powerful combination.

The newest and most convincing version pairs a spoofed number with an artificial voice. Your screen shows a trusted caller, and the voice on the line may be a recording, an AI-generated voice, or even a clone of a real person's voice. Regulators have recognized how dangerous this combination is: the federal communications regulator ruled that using artificial or AI-generated voices in unwanted robocalls is illegal without your consent, giving authorities more tools to go after the worst offenders.

That ruling is good news, but it does not mean the calls have stopped, any more than laws against theft mean no one steals. Criminals break the rules; that is what makes them criminals. So you still receive these calls, now sometimes with a smooth, natural-sounding AI voice that is even more persuasive than a script read by a bored stranger. The faked number earns your trust before you answer, and the faked voice holds it once you do.

Your defense does not change at all, which is the reassuring part. It does not matter whether the voice is a real person, a recording, or a flawless AI clone, because you are not judging the voice any more than you are trusting the screen. You hang up and call back on

a number you look up yourself. The fanciest combination of faked number and faked voice collapses the instant you reach the real organization through a channel you control. The technology on their side cannot touch the number you dial on yours.

GOOD TO KNOW

All voices in unwanted robocalls are illegal without your consent, but scammers ignore the law. So keep verifying by calling back — the rule protects you whether the voice is real, recorded, or cloned.

16. A Note on Scary Voicemails

The threat left on your machine.

Sometimes the spoofed call goes to voicemail and leaves a message, and these can be just as alarming as a live call: a stern voice claiming to be from a government agency or the sheriff, warning of a warrant, a lawsuit, or a suspended benefit, and leaving a callback number with an urgent deadline. Hearing such a message, especially with an official-looking number attached, can set the heart racing and tempt even careful people to call the number back right away.

That callback number is the trap. It does not connect you to the agency; it connects you to the scammer or an accomplice ready to continue the con. So treat a threatening voicemail exactly like a threatening live call: do not call the number it left. If the message worries you enough that you want to be sure, look up the real agency or office yourself and call that, where you will learn the threat was hollow. The voicemail changes nothing about the rule — never use the number the message provides.

It also helps simply to expect these messages and to recognize them for the theater they are. A real agency does not typically leave menacing voicemails demanding instant payment with a countdown. The drama and the urgency are the tells. You can delete such a message with confidence, and if a flicker of doubt remains, resolve it by reaching the real organization through a number you found yourself, calmly and on your own schedule.

WATCH OUT

Never call back the number left in a threatening voicemail. It reaches the scammer, not the agency. Look up the real number yourself if you want to check.

17. If You Already Shared Something

Quick steps to limit the harm.

If a spoofed call already got something from you — a payment, a code, account details, or a transfer to a 'safe account' — take a breath and act promptly, because speed can genuinely help. There is no shame here; you trusted a screen and a voice engineered to be trusted, and catching it now is exactly the right response. The steps depend on what was shared, but moving quickly is the common thread.

- 1 If you moved money or paid, call your bank or card company immediately on the real number, say it was a scam, and ask them to stop or reverse it.
- 2 If you gave a verification code or password, change that password now and turn on the second lock (two-step verification) for the account.
- 3 If you shared card or account numbers, tell the bank so they can watch for or block fraudulent charges.
- 4 Write down the details — the number shown, the time, what was said and shared — while they are fresh.
- 5 Report it to the FCC and the FTC, and ignore any later 'recovery' call offering to get your money back for a fee.

GOOD TO KNOW

The faster you call the bank on its real number, the better your odds. Embarrassment is the scammer's ally — make the call anyway; the fault is entirely theirs.

18. Questions People Ask Me

The ones that come up again and again.

The number on my screen exactly matched my bank's real number — how can that not be them? Scammers often copy a real, published number on purpose, precisely so it matches when you check. A matching number is not proof. The only safe move is to hang up and dial that number yourself, which connects you to the real bank rather than whoever placed the incoming call.

Is it dangerous just to answer a spoofed call? Answering is generally fine; the danger is in what you do next. You can answer, realize it is a scam, and hang up with no harm done, as long as you do not share information, money, or codes. If anything feels off, you owe the caller nothing — just hang up.

How do I know what my bank's real number is? Use the number printed on the back of your debit or credit card, or on a paper statement, or type your bank's web address yourself and find their contact page. Those are numbers you can trust because you found them independently, not because a caller gave them to you.

Can I call back the number that just called me to check? Be careful — if the number was spoofed, calling it back might reach the real owner (an innocent stranger) or, in some setups, the scammers. The reliable method is to ignore the incoming number entirely and look up the organization's official number yourself.

19. A Five-Minute Phone Safety Setup

Quiet settings and notes that do a lot.

A little setup makes the whole spoofing problem easier to live with. None of this is complicated, and it pays off every time a questionable call comes in. Do it yourself or with a hand, and you will feel noticeably more in control of your phone.

- 1 Write your bank's real number (from your card) and other key numbers on a note by the phone.
- 2 Turn on your carrier's free spam-call filtering or app.
- 3 Consider turning on 'silence unknown callers' so only saved contacts ring through.
- 4 Decide, as a settled rule, that you never give money, information, or codes on an incoming call.
- 5 Pick one trusted person you'll call to talk through any call that worries you.

GOOD TO KNOW

The single most powerful 'setting' is a mental one: the screen is a label, not proof. Everything else just makes acting on that truth a little easier.

20. Reporting It — and Why It Helps

A few minutes that protect the next person.

Reporting a scam can feel pointless once the money is gone, but it genuinely matters. Reports help investigators link cases together, give platforms and phone carriers the evidence to shut fakes down, and warn others before they are caught. You do not need to have lost money to report — flagging an attempt is valuable too. It takes only a few minutes, and it turns a bad experience into something that helps your neighbors.

- Report to the Federal Trade Commission at ReportFraud.ftc.gov, the national clearinghouse for scams. You can also call 1-877-382-4357.
- Report online or financial crime to the FBI at ic3.gov, their internet-crime complaint center — especially for larger losses or cryptocurrency.
- Contact the Ohio Attorney General's consumer protection team at 800-282-0515 or through ohioattorneygeneral.gov.
- If your identity may be exposed, visit IdentityTheft.gov for a step-by-step recovery plan.
- Report spam texts by forwarding them to 7726 (SPAM), and use the 'report' button inside apps and email.

I wrote a separate, step-by-step guide on reporting to the FTC, the FBI, and the Ohio Attorney General, with exactly what to write down and what to expect afterward. If the reporting steps feel like a lot, that is a perfect thing to call me about. I am glad to sit with you and help you file, so that your report actually reaches the people who can use it.

GOOD TO KNOW

You will usually not hear back from a report, and that is normal. Your report still joins a bigger picture that helps investigators and warns others, even when nothing lands in your own inbox.

21. When to Just Call Me

A calm second opinion costs you nothing.

If something about a call where the name or number on your screen looks official has you second-guessing yourself, or you just want a steady second opinion before you do anything, please call me. There is never a charge to ask a scam question, and never any judgment. I would far rather spend a few minutes on the phone talking it through with you than hear later that something cost you money or worry. That is genuinely what I am here for, and it is some of the most satisfying work I do.

If you would like a hand in person, I come to homes all across Portage County. I can help you check something safely, tighten up your accounts and passwords after a close call, set your devices and routine so these scams have a harder time reaching you, and walk your whole family through a simple plan. We go at your pace, with no pressure and no rushing, and you come away feeling steadier.

GOOD TO KNOW

The best time to call is before you act — before you click, pay, or share anything. A quick 'does this seem right to you, Bill?' is one of my favorite kinds of call to get.

22. Contact Card & a Warm Close

Keep this page where you can find it again.

Bill's Home Tech — your local tech, Bill Davis, owner and only tech. Phone or text: (330) 200-8042. Email: bill@billshometech.com. Web: billshometech.com. Service area: Atwater, Ravenna, Kent, Streetsboro, Aurora, Rootstown, Mantua, Garrettsville, Windham, Edinburg, Suffield — all of Portage County, Ohio.

- Free phone call: any scam question or close call, always free, with no judgment and no rushing.
- In-home scam-check visit: \$99 flat for the first visit, with a 30-day follow-up included.
- Remote help by screen-share, for when you would rather not wait for a visit.

The number on your screen is a label anyone can print — never proof of who is really calling. Hang up on anything that rushes you for money or information, and call back on a number you look up yourself. If you ever want help setting up call filtering or just talking a call through, I am a phone call away and glad to help.

CHEAT SHEET

Everyday Cheat Sheet

The one rule

Caller ID can be faked. The screen is a label, not proof. Hang up and call back on a number you look up yourself.

Common disguises

- Your bank's 'fraud department.'
- IRS, Social Security, or Medicare 'problems.'
- The sheriff, with a warrant or missed jury duty.
- A familiar local-looking number.
- A 'security' call wanting a verification code.

Do this, every time

- 1 Don't trust the name or number on the screen.
- 2 Never use a number the caller gives you.
- 3 Hang up; look up the real number yourself.
- 4 Call back on that number and confirm.
- 5 Never share money, info, or a code on an incoming call.

WATCH OUT

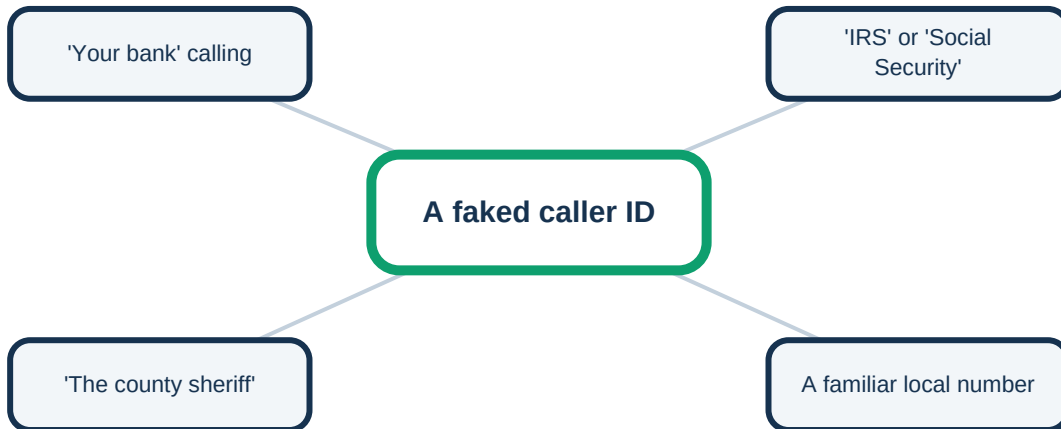
'Read me the code' and 'move your money to a safe account' are always scams — no real bank, agency, or officer ever asks for either.

AT A GLANCE

A Picture to Follow Along

Why the Screen Can't Be Trusted

Anyone can print any name or number on your caller ID.



The number is a label anyone can set - never proof of who calls.

Illustration - a schematic; details vary by device and setup.

AT A GLANCE

A Second Look

The Habit That Beats Spoofing

Leave the incoming call; reach the real org yourself.

- 1 A trusted name shows and pressures you
- 2 Remember: the screen is a label, not proof
- 3 Share no money, info, or codes
- 4 Hang up - don't use the caller's number
- 5 Look up the real number yourself (card/site)
- 6 Call back there and confirm

They control the call in - not the number you dial out.

Illustration - a schematic; details vary by device and setup.

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

In-home visit — \$99 flat for your first visit. No contracts and no surprise charges, and a 30-day follow-up is included.

Remote Support — \$49 for a screen-share session. I only connect with your permission, you watch the whole time, and you can end anytime. If I can't fix it over the screen-share, I refund the \$49 — and if it turns out you need me in person, that \$49 goes toward your visit. It's included free for Support Plan members (\$39/mo).

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.

Call or text **(330) 200-8042** · Book a visit: **billshometech.com/book** · **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.