



The Verify-First Habit — The One Rule That Beats Every AI Fake

One simple family habit that beats even a perfect fake.

————— An Extended Guide · No. 1635 · 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. Why Spotting Fakes No Longer Works	5
3. What 'Verify First' Means	6
4. Why It Beats Even a Perfect Fake	7
5. The Four Ways to Verify	7
6. Make It Automatic With a Trigger	8
7. The Pause Is the Hard Part	9
8. A Script to Buy Yourself the Pause	10
9. The Two Channels to Never Trust	11
10. Making It a Family Rule	11
11. How It Handles Each Kind of Scam	12
12. It Works Against Tomorrow's Scams Too	13
13. Overcoming the Awkwardness	14
14. Teaching Children and Grandchildren	15
15. When You Can't Verify Right Away	16
16. Building the Habit Into Your Day	16
17. Trust the Little Voice, Too	17
18. Questions People Ask Me	18
19. A Five-Minute Family 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

You cannot reliably spot every fake anymore — voices, faces, emails, and caller ID can all be forged. So stop trying to judge whether a request is real, and instead verify it. The habit: before you act on any urgent request for money, information, or access, you confirm it through a separate channel you already trust — a callback to a known number, a question only the real person could answer, or a family safe word. One rule, used every time, beats every fake, even a perfect one.

- 1 An urgent request arrives — money, a code, account access, a secret.
- 2 Don't judge whether it looks or sounds real; assume it might be fake.
- 3 Stop before acting.
- 4 Verify on a separate channel you already trust — not the one that contacted you.
- 5 Act only after you've confirmed it independently.

GOOD TO KNOW

This works because you control the channel you verify on, but the scammer controls the one that reached you. That's why verifying beats spotting — it doesn't depend on catching the fake.

1. Why I Wrote This One

One habit to replace a hundred warnings.

In more than thirty years of helping people across Portage County with their technology, I have written and taught about more scams than I can count. And I have come to believe that the most useful thing I can give anyone is not a list of a hundred scams to memorize, but a single habit that beats nearly all of them — including the new ones and the ones not yet invented. This guide is about that one habit, which I call verify first.

Here is the problem it solves. Scammers can now fake almost everything we used to rely on: a loved one's voice on the phone, a familiar face on a video call, a flawless email from your bank, the number and name on your caller ID. The old advice — listen for the robotic voice, watch for bad spelling, trust the caller ID — has quietly stopped working, because the fakes have gotten too good. Trying to spot each fake is a game you will increasingly lose as the technology improves.

The verify-first habit sidesteps that losing game entirely. Instead of trying to judge whether something is fake — which is hard and getting harder — you simply confirm any urgent request through a separate channel you already trust, before you act. You stop being a fake-detector and become a verifier, and verifying is something anyone can do reliably, no technical skill required. We will unpack why it works, how to make it automatic, and how to build it into your whole family's life as a calm, shared norm.

WATCH OUT

If you only teach your family one thing about scams, make it this habit. It covers voice clones, deepfakes, phishing, impostor texts, and scams that don't exist yet.

2. Why Spotting Fakes No Longer Works

The ground has shifted under the old advice.

It is worth being honest about why the advice many of us grew up with has failed, because that honesty is what motivates the new habit. For years, scams gave themselves away: a stilted robocall voice, broken English in an email, a crude fake website, a stranger who could not possibly sound like your grandchild. We learned to spot those tells, and for a long time, spotting worked well enough. That era is ending.

Artificial intelligence has erased the tells. It writes flawless, natural emails in any language. It generates lifelike voices and can clone a specific person's voice from seconds of audio. It can fake a familiar face on a live video call. Caller ID has long been easy to forge. One by one, the signals we used to judge a contact's authenticity have become unreliable, because the fakes now look and sound exactly like the real thing. Spotting the fake is no longer a skill you can count on.

This is not cause for despair, but for a change of strategy. When you cannot tell the real from the fake by looking and listening, you stop trying to, and you shift to a method that does not depend on your senses at all. That method is verification through a trusted channel, and it works precisely because it ignores the thing the scammer controls — the appearance of the contact — and relies instead on something the scammer cannot touch. The ground has shifted, so our habit must shift with it.

GOOD TO KNOW

Every old 'tell' — robotic voice, bad grammar, odd caller ID — has been erased by AI. That's not a reason to despair; it's a reason to verify instead of trying to spot.

3. What 'Verify First' Means

The habit, stated plainly.

Let me state the habit as plainly as I can, because its power is in its simplicity. Verify first means: before you act on any urgent or unexpected request for money, personal information, account access, or secrecy, you confirm that request through a separate channel you already trust — regardless of how the request reached you or how real it seems. Only after you have independently confirmed it do you act. That is the whole rule.

Three words in that rule carry the weight. 'Separate' means the channel you verify on must be different from the one that contacted you — you do not verify a suspicious call by staying on that call, or a suspicious text by replying to it. 'Trust' means it is a channel you already rely on — a phone number you have had for years, an app you installed yourself, an in-person conversation. 'Already' means you are not using any number, link, or contact the suspicious message provided, since those lead back to the scammer.

So verify first is not about interrogating the person who contacted you or testing them with questions. It is about leaving their channel entirely and reaching the real party another way. If 'your bank' calls, you hang up and call the number on your card. If your 'grandchild' texts for money, you call their known number. If your 'boss' emails to wire funds, you confirm in person or on a known line. Same simple move, every time: step outside the contact, and confirm on a channel you already trust.

WATCH OUT

The three key words: SEPARATE channel (not the one that reached you), that you TRUST, and that you ALREADY had (never a number or link they gave you).

4. Why It Beats Even a Perfect Fake

The reason this one habit is enough.

The deep reason verify first works is worth understanding, because understanding it is what lets you trust it completely. Every scam, whatever its disguise, reaches you through a channel the scammer controls — the call they placed, the text they sent, the email they wrote, the video meeting they set up. They can make that channel look and sound flawless. But there is one thing they cannot control: a separate channel that you choose and already trust.

When you verify through that separate channel — dialing your grandchild's real number, logging into your bank the way you always do, asking a question only the real person could answer — you step completely outside the scammer's reach. It does not matter how perfect their fake was, because you are no longer relying on it. You have moved the decision onto ground the scammer cannot touch. This is why verify first beats even a flawless fake: it does not try to out-detect the fake, it simply refuses to act on the scammer's channel at all.

Contrast that with trying to spot the fake, which pits your eyes and ears against the scammer's technology — a contest that gets harder every year as the fakes improve. Verify first takes you out of that contest entirely and onto ground where you always win, because a real request confirms itself on your trusted channel and a fake one simply cannot. That permanence is the beauty of it: no matter how good the fakes get, verifying on a channel you control will keep working.

GOOD TO KNOW

Spotting fakes pits you against the scammer's technology — a losing contest. Verifying moves the decision onto ground they can't touch — a contest you always win.

5. The Four Ways to Verify

Your toolkit for confirming anything.

Verifying is simple, and there are really just a few trusted channels you will ever need. Keep these four in mind and you can confirm almost any suspicious request. Each one is a separate channel the scammer does not control, and you can pick whichever fits the situation.

- The callback: hang up and call the person or organization on a number you already have — the back of your card, your saved contacts, an official website you type yourself.
- The known app or login: reach your bank or a service the way you always do, through its app or your saved bookmark, never a link they sent.
- The safe word: ask for a private family word an outsider couldn't know — perfect for an urgent 'loved one in trouble' call.
- The personal question or in-person check: ask something only the real person would know, or simply confirm face-to-face or with someone who's with them.

Which one you reach for depends on the situation. A call from 'the bank' calls for the callback or the known app. A frightening 'grandchild in trouble' call calls for a callback to their real number, with the safe word as backup if you cannot reach them. A 'boss' urgently requesting a transfer calls for an in-person check or a call to a known number. In every case, the move is the same in spirit: leave the suspicious contact and confirm on one of these trusted channels.

TIP

Four tools cover almost everything: call a known number, use the real app, ask the family safe word, or confirm in person. Pick whichever fits the moment.

6. Make It Automatic With a Trigger

What should make the habit fire.

A habit only protects you if it fires at the right moment, so it helps to know exactly what should trigger verify first. The trigger is a specific combination, and once you learn to recognize it, the habit kicks in almost on its own. The trigger is: an urgent or unexpected request for money, personal information, account access, or secrecy. When you notice that combination, the habit says: stop, and verify before acting.

Let me make the trigger concrete. It fires when a call, text, email, or message wants you to send money, pay a bill or fee, buy gift cards, share a password or verification code, confirm personal or account details, grant access to your computer, or keep something secret from family — especially when it presses you to do so quickly. Any one of those, arriving unexpectedly or from an unexpected source, is your cue. You do not have to decide if it is a scam; you just have to recognize the trigger and verify.

What does not need to trigger it is just as important, so the habit does not make you anxious about everything. An ordinary chat with your grandchild on their usual number, a newsletter you subscribed to, a call you placed yourself to a company — none of these involve an unexpected demand for money, information, or secrecy, so they sail through normally. The trigger is specific, which means you can relax most of the time and reserve the verify-first habit for the narrow, recognizable situations that actually carry risk.

TIP

The trigger to memorize: an unexpected request for money, info, access, or secrecy — especially if rushed. That combination means 'stop and verify.' Everything else, relax.

7. The Pause Is the Hard Part

Why urgency is designed to skip it.

The single hardest moment in verify first is the pause — the beat between feeling the urge to act and actually acting. Scammers know this, which is why nearly every scam manufactures urgency: act now, there's no time, you'll lose everything, they're waiting. All that pressure exists for one purpose: to eliminate the pause, because a person who pauses is a person who might verify, and a person who verifies cannot be scammed.

So the heart of the habit is giving yourself permission to pause, always, no matter how urgent the request feels. A real emergency survives a sixty-second pause; a real opportunity survives a day's thought; a real institution does not punish you for taking a moment to confirm. The urgency itself is a warning sign, not a reason to hurry. When you feel most rushed is exactly when you most need to stop, because that pressure is the scammer's main tool, deliberately applied.

It helps enormously to decide, calmly and in advance, that you will always take the pause — to make it a settled personal rule rather than a decision you try to make under pressure. 'I always pause and verify before acting on an urgent money request' is a commitment you make once, in a quiet moment, and then simply execute when the time comes. A rule set ahead of time holds when feelings waver, which is precisely when you need it to hold.

WATCH OUT

Manufactured urgency exists to kill the pause. So feeling rushed is itself the signal to slow down — the more a request insists 'act now,' the more it needs you to verify.

8. A Script to Buy Yourself the Pause

Words that make stopping easy.

Because the pause is hard, it helps to have ready-made words that let you step out of a pressured moment without feeling rude or flustered. Scammers rely on social pressure — the awkwardness of hanging up, of saying no, of doubting someone who sounds official or like a loved one. A prepared phrase dissolves that awkwardness and gives you an easy, guilt-free exit to go and verify.

- 'Let me call you right back.' — then hang up and verify. You owe no explanation.
- 'I never make money decisions on the spot; I'll check and get back to you.'
- 'I don't share codes or account details on calls I didn't place.'
- 'If this is real, it'll still be real after I confirm with my bank/family.'
- 'No, thank you.' — a complete answer that needs no justification.

None of these require arguing, proving anything, or being unkind. They simply end the pressured moment and hand you the pause you need. A legitimate caller or request will survive any of them without trouble — a real bank is fine with you calling back, a real loved one is fine with you confirming. Only a scammer pushes back against these words, and that pushback is itself confirmation that stepping away to verify was exactly right.

Practice your favorite line out loud a few times when nothing is wrong, so it comes easily when you are under pressure. The goal is for the words to be automatic, so that in the heat of a convincing scam, you reach for them without having to think. A phrase your mouth already knows is one of the most practical defenses there is, because it gets you to the pause, and the pause gets you to verification.

WATCH OUT

Keep one line ready: 'Let me call you right back.' Say it, step away, and verify. It's the simplest way to claim the pause the scam is trying to deny you.

9. The Two Channels to Never Trust

Where NOT to verify.

Verify first only works if you verify on the right channel, so it is crucial to know the two channels you must never use to confirm a suspicious request. Getting this wrong is the most common way people think they have verified when they actually have not, so it is worth stating clearly.

First, never verify through the same channel that contacted you. If a caller claims to be your bank, do not 'confirm' by asking that caller to prove it — of course they will say they are the bank. If a text claims to be your grandchild, do not reply to that text to check — the scammer will insist they are your grandchild. The suspicious channel is controlled by the scammer, so any confirmation it offers is worthless. You must leave it entirely.

Second, never use a number, link, website, or contact that the suspicious message itself provided. Scammers helpfully give you a 'bank fraud line' to call back, a 'secure link' to click, an email address to write to — all of which lead straight back to them or their accomplices. A callback number in a threatening voicemail, a link in a phishing text, a phone number read out by a 'government official' — none of these are safe. Always find the real contact yourself, independently, from a source you already trust. Those two 'never' rules are what make verification genuine rather than an illusion.

WATCH OUT

You haven't verified if you used the same channel that contacted you, or a number/link it gave you. Both lead back to the scammer. Always confirm on a channel you found yourself.

10. Making It a Family Rule

The habit spreads best shared.

Verify first is powerful for one person, but it becomes a fortress for a whole family, because scams that exploit family bonds — a cloned grandchild, a hacked relative's account, an impostor child texting — only work if someone in the family acts without verifying. When every family member shares the habit, there is no weak link to find. So the most protective thing you can do is make verify first a shared family norm, not just your own private caution.

Have one short, warm conversation, ideally at a relaxed family gathering. Agree together on the simple rule: nobody in the family acts on an urgent money, information, or secrecy request without verifying it on a trusted channel first, and nobody is ever annoyed or embarrassed by that check. Set up the tools that make it easy — a family safe word, everyone's real numbers saved in each other's phones, a shared understanding that a real number change is confirmed by a call, not sprung in a money text.

Frame it as something the whole family does together, equally, so no one feels singled out as the one who 'needs protecting.' The grandchildren adopt it as much as the grandparents; the tech-savvy adopt it as much as those less comfortable with devices, because the fakes fool everyone. When verify first is simply how your family operates — a normal, shared, no-judgment habit — your family becomes remarkably hard to scam, in every direction across the generations.

GOOD TO KNOW

A family where everyone verifies has no weak link for scams to find. Make it a shared norm — grandkids and grandparents alike — so no one feels singled out.

11. How It Handles Each Kind of Scam

One rule, many disguises.

The joy of verify first is that one habit handles an enormous range of scams, so you do not have to learn a separate defense for each. It is worth seeing how the single rule maps onto the common threats, because that mapping shows you how much ground one habit covers.

- Voice-cloning call ('grandchild in trouble'): hang up, call their real number, or ask the safe word.
- Deepfake video call (an urgent transfer): confirm with the real person on a known channel before acting.
- Bank or government impersonation call: hang up, call the number on your card or the agency's official line.
- Phishing email or text: don't click; reach the company through its app or your bookmark.
- Impostor 'new number' text: call the old, saved number to confirm.
- An online friend urging an investment: verify independently, and never act on a relationship that began online.

Notice that the specifics differ a little, but the shape is identical every time: do not act on the suspicious contact; confirm through a separate channel you already trust. Once you internalize that shape, you do not need to recognize which particular scam you are facing. You only need to recognize the trigger — an unexpected, urgent request for money, information, access, or secrecy — and then verify. The one habit does the rest, whatever costume the scam is wearing.

WATCH OUT

You don't need to identify which scam you're facing. Recognize the trigger — urgent request for money, info, access, or secrecy — and verify. One habit covers them all.

12. It Works Against Tomorrow's Scams Too

Why this habit is future-proof.

One of the best things about verify first is that it protects you against scams that do not exist yet. New frauds appear constantly, powered by new technology, and no one can keep up with a list of them all. But because verify first does not depend on recognizing a specific scam — it only depends on the universal trigger and the universal response — it works just as well against a brand-new scam as against a familiar one. You do not have to have heard of a scam to be protected from it.

Consider how much the landscape has already changed. A few years ago, voice cloning and live deepfake video calls were science fiction to most people; now they are real tools in scammers' hands. Whatever comes next — and something will — it will still, almost certainly, need to make an urgent request for money, information, access, or secrecy through some channel it controls. And verify first will still answer it the same way: step outside that channel and confirm on one you trust. The habit is future-proof in a way that no list of scams can be.

This is why I value teaching the habit far more than teaching any particular scam. Scams come and go and mutate; the habit endures. A family that has truly internalized verify first does not need to be re-taught with every new fraud that makes the news. They are already protected, because they respond to the shape of a scam, not its specific disguise. In a world where the fakes keep getting better, that durable, general defense is worth more than any amount of scam-spotting.

GOOD TO KNOW

You don't need to have heard of a scam to be protected from it. Verify first answers tomorrow's frauds the same way it answers today's — because it responds to the shape, not the disguise.

13. Overcoming the Awkwardness

Giving yourself permission to doubt.

A real barrier to verify first is social: it can feel rude or distrustful to hang up on someone, to doubt a loved one's voice, or to question an official or a boss. Scammers exploit this politeness ruthlessly, counting on your reluctance to be 'difficult.' So part of building the habit is giving yourself explicit permission to verify, every time, without guilt — and understanding that doing so is not rude at all, but simply sensible in the world we now live in.

Reframe it in your mind. Verifying is not an insult to anyone; it is a normal, reasonable precaution, like locking your door or wearing a seatbelt. A genuine loved one, a real bank, an honest company, a decent boss — none of them will be hurt or offended by your taking a moment to confirm an important request, and most will respect you for it. The only party ever bothered by your verifying is a scammer, whose whole scheme depends on your not doing it.

It also helps to make verifying a known, expected norm among the people you deal with, so there is no awkwardness at all. When your family has agreed that everyone verifies and nobody minds, there is nothing uncomfortable about a callback. When your workplace has a policy that all transfers are confirmed, no employee feels they are doubting the boss. Normalizing the habit, out loud and in advance, removes the social friction that scammers rely on, and makes verifying the easy, natural thing to do.

GOOD TO KNOW

Verifying isn't rude — it's a sensible precaution, like locking a door. Only a scammer is ever bothered by it. Give yourself permission to confirm, every time, guilt-free.

14. Teaching Children and Grandchildren

The habit is for every generation.

Verify first is not just for older adults; it is for everyone, and teaching it to children and grandchildren protects both them and you. Young people are targeted by scams too — fake job offers, prize and gaming scams, social-media account takeovers, romance and investment cons — and their confidence that they could never be fooled often makes them more vulnerable, not less. A grandchild who learns verify first is safer in their own life and better able to help protect the family.

Teach it to them as a life skill rather than a fearful warning. The principle is empowering: you do not have to be suspicious of everyone or scared of your phone; you just confirm anything important through a channel you trust before acting. Frame it as savvy and grown-up, which lands well with younger people, and connect it to things they care about — protecting their accounts, their money, and the grandparents they love, whose voices could be cloned using the family's own videos.

Make it a two-way exchange that strengthens the whole family. Let the grandchildren teach the older members about the newest apps and how their settings work, while the older members share the hard-won wisdom that the fanciest fake still falls to a simple verification. When every generation holds the same habit, the family's defenses are seamless, and the habit passes down as naturally as any other piece of family know-how. That shared, cross-generational practice is the real prize.

TIP

Teach kids verify first as a savvy life skill, not a fear. It protects their accounts and money now, and makes them allies in protecting the grandparents they love.

15. When You Can't Verify Right Away

The safe default: do nothing yet.

Occasionally you will face an urgent request and be unable to verify immediately — you cannot reach the person, it is the middle of the night, the office is closed. Scammers love these moments and will insist the impossibility of checking means you must act now on their say-so. It means the opposite. When you cannot verify, the safe default is simple: you do nothing yet. You do not send money, share information, or grant access until you can confirm.

This is where a family safe word earns its keep, giving you a way to verify a 'loved one in trouble' even when you cannot reach them by callback. But absent any way to confirm, waiting is not just acceptable — it is the correct and safe choice. Nearly every genuine situation can wait the hours it takes until you can verify in the morning, reach the person, or consult someone you trust. The handful of things that truly cannot wait are real emergencies best served by calling 911, never by wiring cash to a caller.

So make peace with the power of 'not yet.' A scammer frames the inability to verify as a reason to skip verifying; you flip that completely and treat it as a reason to wait. 'I can't confirm this right now, so I'm not going to act until I can' is a complete, safe, and entirely reasonable position, and no legitimate request is harmed by it. When in doubt and unable to check, doing nothing is doing exactly the right thing.

WATCH OUT

Being unable to verify is never a reason to act anyway — it's a reason to wait. 'I can't confirm this, so not yet' is a safe, complete answer. Real things survive the wait.

16. Building the Habit Into Your Day

Small reminders that make it stick.

Like any habit, verify first sticks best with a few gentle reminders and supports, especially while it is still new. You do not have to rely on willpower or memory alone; a little setup keeps the habit in front of you until it becomes second nature. These small touches make the difference between knowing the rule and actually using it in the heat of a convincing scam.

- Write the rule on a card by the phone and computer: 'Urgent request? Verify first — call a number I already have.'
- Save your key real numbers — bank, family, doctor — so a verifying callback is one tap away.
- Set your family safe word and make sure everyone knows it.
- Keep a short list of your 'call first' people — who you'll check with before acting.
- Talk about it now and then, sharing scam stories, so it stays fresh and normal.

The physical card by the phone is especially valuable, because the moment you most need the habit — under the pressure of a convincing scam — is the moment memory fails. A card you can glance at, that simply says 'verify first,' can be enough to break the spell and remind you to pause and confirm. It costs nothing and asks nothing of your memory at the critical instant.

Over time, the reminders become unnecessary, because the habit takes hold. You will find yourself instinctively reaching to call back, to confirm, to pause, without having to think about it. That is the goal: verify first woven so deeply into how you handle urgent requests that it protects you automatically, like looking both ways before crossing a street. Until then, lean on the cards and the reminders, and be patient with yourself as the habit settles in.

WATCH OUT

A card by the phone that just says 'Verify first — call a number I already have' can break a scam's spell at the exact moment memory fails. Cheap, simple, powerful.

17. Trust the Little Voice, Too

Your instincts are an ally of the habit.

While verify first is designed so you do not have to rely on spotting fakes, your own instincts are still a valuable ally, and it is worth honoring them. Often, before you can put your finger on anything, a small inner voice says 'something about this feels off.' That feeling is your experience and intuition working below the surface, catching a wrongness you have not yet consciously named. In the world of scams, that quiet unease is almost always worth listening to.

The beauty is that you do not have to justify the feeling or prove anything to act on it. If a request makes you uneasy, that unease alone is reason enough to pause and verify — you need no better evidence than your own discomfort. Scammers count on people overriding

that instinct out of politeness, urgency, or self-doubt ('I'm probably just being paranoid'). So treat the little voice not as paranoia to suppress but as a prompt to run the habit you already have.

At the same time, the habit protects you even when your instincts are silent, which is its great strength. Some scams feel entirely smooth and raise no inner alarm at all, which is exactly why you tie verify first to the objective trigger — an urgent request for money, information, access, or secrecy — and not only to your gut. So use both: let your instincts trigger the habit when they fire, and let the objective trigger fire it even when they do not. Between the two, very little gets past you.

GOOD TO KNOW

If something feels off, that unease alone is reason enough to verify — you never have to justify it. And the objective trigger protects you even when your gut stays quiet.

18. Questions People Ask Me

The ones that come up again and again.

Isn't it exhausting to verify everything? You don't verify everything — only the specific trigger: an unexpected, urgent request for money, information, access, or secrecy. That's a narrow slice of your day. Ordinary calls, texts, and chats sail through normally. The habit lets you relax the rest of the time, precisely because you know when to be careful.

What if verifying offends a real person or my boss? It won't offend anyone genuine. A real loved one, bank, company, or boss accepts a confirmation without trouble, and most respect it. Only a scammer is bothered by your verifying. If you normalize the habit out loud in your family and workplace, there's no awkwardness at all.

The request came from a number and name I recognized — do I still verify? Yes, because caller ID, email addresses, and even hacked real accounts can all be faked or compromised. A familiar source is reassuring but not proof. If it's an urgent request for money, info, access, or secrecy, verify through a separate trusted channel regardless of how familiar the source looks.

Isn't this just common sense? It is — but common sense that the old 'spot the fake' advice quietly replaced, and that scammers work hard to override with urgency and polish. Naming it, practicing it, and making it a shared family rule turns loose common sense into a

reliable habit that actually fires when you need it.

19. A Five-Minute Family Setup

Make verify first your family's rule today.

Here is how to put the one habit in place for your whole family in about five minutes. Do it together at a relaxed moment, keep it light, and you will have given everyone a defense that covers today's scams and tomorrow's alike. This single setup is worth more than memorizing any number of individual scams.

- 1 Agree on the rule: no one acts on an urgent request for money, info, access, or secrecy without verifying on a trusted channel first.
- 2 Agree nobody is ever annoyed or embarrassed by a verification — it's just how the family operates.
- 3 Set a family safe word: private, odd, never posted online.
- 4 Make sure everyone's real numbers are saved in each other's phones.
- 5 Write 'Verify first — call a number I already have' on cards by the phones.
- 6 Teach every generation, grandkids included, and revisit it now and then.

GOOD TO KNOW

This one setup replaces a hundred scam warnings. A family that verifies first is protected against voice clones, deepfakes, phishing, impostor texts — and whatever comes next.

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](https://www.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](https://www.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 building a 'verify first' habit for your whole family 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.

One calm habit — verify on a channel you trust before you act — protects your family against scams that haven't even been invented yet. Set it up together, keep it light, and call me anytime you'd like help. I am a phone call away, and always glad to help a family stay safe.

CHEAT SHEET

Everyday Cheat Sheet

The one rule

Before acting on any urgent request for money, information, access, or secrecy, verify it on a separate channel you already trust.

The trigger

- An unexpected request for money or a fee.
- A request for a password, code, or account details.
- A request for access to your computer.
- Pressure to act now, or to keep it secret.
- Any of these, however real the source looks.

How to verify

- 1 Don't act on the contact that reached you.
- 2 Call a number you already have (not one they gave).
- 3 Or use the real app / your saved bookmark.
- 4 Or ask the family safe word.
- 5 Can't verify yet? Do nothing until you can.

GOOD TO KNOW

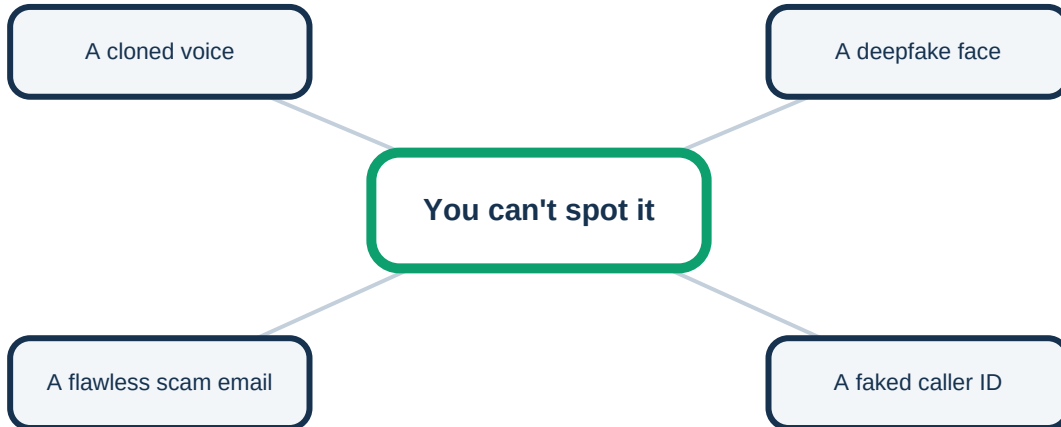
You haven't verified if you used the same channel that contacted you, or a number or link it provided. Always confirm on a channel you found yourself.

AT A GLANCE

A Picture to Follow Along

Stop Spotting, Start Verifying

The fakes are too good to catch by eye or ear.



So don't try - verify on a channel you already trust.

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

AT A GLANCE

A Second Look

The Verify-First Habit

One move that beats every fake, even a perfect one.

- 1 An urgent request for money, info, or access arrives
- 2 Don't judge if it's real - assume it might be fake
- 3 Stop before acting
- 4 Leave that channel; confirm on one you trust
- 5 Use a known number, the real app, or a safe word
- 6 Act only after you've confirmed independently

They control the channel that reached you - not the one you verify on.

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.