



An Extended Guide · No. 2069

The Fake Invoice & "New Bank Details" Scam: A Call-Back Rule That Stops It

A one-page verification rule that
beats payment-redirection fraud

Tech Made Simple — Service Made Personal

BillsHomeTech.com · (330) 200-8042 · Atwater, Ohio

Free & printable — share it with someone who needs it



Book a visit —
billshometech.com/book

! Read this first — the two things that stop most attacks

Almost every small-business break-in starts in one of two ordinary ways: a password that got stolen or guessed, or a convincing email that talked someone into clicking or paying. You do not have to become a computer expert to stop most of it. Turn on two-step sign-in (also called multi-factor authentication, or MFA) everywhere you can, keep a backup you have actually tested, and give yourself permission to slow down before you click a link, open an attachment, or send a payment. That is the whole game, most days. This guide is about that second habit — slowing down before you pay — because the costliest scam hitting small businesses isn't fancy hacking at all. It's a convincing email asking you to send money to the wrong place.

The scam that empties bank accounts with no hacking at all

A vendor emails new bank details for their next payment. A boss emails asking you to wire money, quickly and quietly. An invoice lands that looks just like the real ones. Pay it, and the money is gone — to a crook, not your vendor. This guide gives you one simple rule that stops it cold.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. I've spent 30+ years helping folks and small businesses stay out of trouble with their technology, in plain language. This is one of the most important guides I've written, because this scam is quietly one of the costliest crimes hitting small businesses.

The good news: there's no malware to fight here. It's a trust-and-process problem, and the fix is a process — a short, out-loud rule everyone who touches money follows, every time. Once it's in place, this scam stops working on you.

★ I'll help you write the rule and post it by the desk

In one visit I can help you set up the call-back rule, write it on a single card for whoever pays bills, and tighten your email so the fakes are easier to spot. Call or text me at (330) 200-8042.

The whole guide, on one page

If you remember only these things, you'll beat this scam.

- ❑ Any **change to payment details** or any **new wire request** gets verified before you pay — no exceptions.
- ❑ Verify by **calling a known number you already had on file** — never the number or email in the request itself.
- ❑ Have a **second person** approve payments over an amount you pick.
- ❑ Red flags: **urgency, secrecy, a new account, 'don't call just email,'** and slight changes to an email address.
- ❑ Slowing down is the whole defense. The crook is counting on you being busy and polite.
- ❑ If money already went out, act fast — call your bank now and report to the FBI at **ic3.gov**.

! The request that rushes you is the one to slow down on

Every version of this scam leans on urgency — a deadline, an angry boss, a vendor who'll 'charge a late fee.' That pressure is not a reason to hurry; it's the single biggest sign to stop and verify. Real partners understand a quick call-back.

How the scam actually works

It helps to see the crook's playbook, because it's the same every time once you know it.

This family of scams goes by the name **business email compromise**, or BEC. A crook poses as someone you trust — a vendor, your boss, a contractor, even an employee — and sends a message designed to redirect a payment into their account. Sometimes they've actually broken into a real email account; sometimes they just fake the name and a lookalike address.

The message is ordinary on purpose. 'We've switched banks — please update our details for the next payment.' 'Can you get this wire out before end of day?' 'Here's the invoice, same as always.' Nothing explodes, nothing looks hacked. You simply pay the wrong account, and by the time anyone notices, the money has moved on.

! No malware, no alarm bells — that's why it works

This isn't a virus you can scan for. It's a confidence trick that turns your own helpfulness and hurry against you. The only reliable defense is a habit: verify payment changes a different way before you act.

The red flags to train your eye on

Learn these, and most attempts will trip an alarm in your head before they ever reach your bank.

- **Urgency:** a tight deadline, a late fee, a boss who needs it 'right now.' Pressure is the scam's favorite tool.
- **Secrecy:** 'keep this between us,' 'I'm in a meeting, just handle it.' Real requests survive a second set of eyes.
- **A new account:** any request to change where money goes — new bank, new routing number — is the highest-risk request there is.
- **'Don't call, just email':** the crook steers you away from the one thing that would catch them — a phone call.
- **A slightly-off email address:** a letter swapped, a '.co' instead of '.com,' an extra word in the domain.
- **A tone that's a little off:** a vendor who's suddenly formal, a boss who's suddenly casual.

✓ One red flag is enough to stop and verify

You don't need to spot all six. Any single one of these is reason enough to pause and run your call-back rule. The whole point is that you never have to be sure it's a scam — you just have to verify before you pay.

The call-back rule, in one sentence

Here's the entire defense, and it fits on an index card.

Before you change any payment details or send any new or unusual payment, verify the request by calling a phone number you already had on file — not a number from the message — and have a second person sign off. That's it. Say it out loud, post it by the desk, and make it the rule nobody skips.

Security folks call this **out-of-band verification**: you confirm the request through a different channel than the one it came in on. The request came by email, so you verify by phone — using contact details you trust, from your own records, not from the email.

! Never use the number in the message

This is the heart of it. If the email came from a crook, so did the phone number, the 'updated contact,' and the reply-to address in it. Call the vendor at the number on last month's invoice or in your own contacts — the one you know was good before any of this started.

Why the number has to come from your own records

This one detail is what separates a rule that works from one that just feels safe.

A clever scam email will often include a phone number and invite you to 'call to confirm.' That's a trap. Call it and you reach the crook, or an accomplice, who cheerfully confirms the fake details. You've done a verification step and gotten a false sense of safety.

So the rule is strict on purpose: the number you call must come from **before** this request — a past invoice, the contract, the number saved in your phone from months ago, the vendor's main line on their official site. If the only place you can find the number is the suspicious message, you haven't verified anything.

✓ Keep a short trusted-contacts list

For your handful of regular vendors and your bank, keep a simple list of known-good phone numbers somewhere steady — not in the email thread. Then verifying is a ten-second lookup, and there's never a temptation to use the number the scammer helpfully provided.

A second person, for payments over a line you draw

The call-back catches most of it. A second approver catches the rest — and takes the weight off any one person.

Pick a dollar amount that makes sense for your business, and make it a rule that any payment above it — and **any** change to bank details, at any amount — needs a second person to approve. Two people rarely get fooled by the same trick on the same day, and it means no single employee is left alone carrying a scary decision.

This isn't about distrust. It's the same reason two people count the cash drawer. It protects your staff as much as your money: if a payment ever goes wrong, nobody's hung out to dry for a judgment call they made alone under pressure.

✓ Make it safe to say 'let me check'

The scam works partly because people are afraid to question a request that seems to come from the boss or a big client. Tell your team, plainly and often, that you will never be upset by a call-back — and that 'let me verify that' is always the right answer, never a rude one.

The one-page procedure to post by the desk

Here's the whole thing as a short checklist anyone who pays bills can follow, every time.

- ❑ A request asks to **change payment details** or send a **new or unusual payment**? Stop here and verify.
- ❑ Find a **known-good phone number** from your own records — past invoice, contract, saved contact. Not from the message.
- ❑ **Call and confirm** the exact details with a real person you reach at that number.
- ❑ For anything over your set amount, or any bank-detail change, get a **second person to approve**.
- ❑ Only then make the payment, and **note who verified it and how**.
- ❑ Something feels off even after all that? **Don't pay**. A real partner will wait a day for you to be sure.

★ Want this as a printed card for the desk?

I'll help you turn this into a clean one-page card tailored to your business — your approval amount, your vendors' real numbers — and post it wherever bills get paid. Call (330) 200-8042.

A few extras that make you even harder to fool

The call-back rule is the main event. These quiet habits make the fakes easier to catch in the first place.

- **Turn on MFA for email** so a crook can't log into a real account and send from inside it — see our Microsoft 365 and Google Workspace sign-in guides.
- **Hover over the sender** and read the full address, not just the display name. The lookalike is often one character off.
- **Be wary of reply-to tricks:** the message looks like a normal thread, but replies quietly go to the crook.
- **Confirm big changes in person or by a known number** even from your own staff — their account could be the one compromised.
- **Watch for 'the usual' invoices with a new account number** — same logo, same layout, different bank.

✓ Display names lie; addresses are harder to fake

Anyone can set the name that shows up as 'Your Vendor, Inc.' The actual email address and the real destination of a reply are much harder to fake convincingly. Train your eye to check those, not the friendly name.

Who pays the bills changes how you set this up

The call-back rule is the same everywhere, but how you put it in place depends on whether you pay every bill yourself or have staff who do.

If you're the owner who pays every bill

When it's just you, you are the whole process — which means the discipline has to live in your own habits, because there's no second person to catch a bad day.

- Make the call-back rule a personal non-negotiable: no payment change goes out without a call to a known number first.
- Line up a trusted second person — a spouse, partner, or your accountant — to sign off on big or unusual payments.
- Keep your trusted-contacts list handy so verifying is quick and you're never tempted to skip it when you're slammed.
- Turn on MFA for your email first; if your own account gets taken over, the scam gets far more convincing.

If you have a bookkeeper or staff who pay

When other people touch money, the rule has to be written down, taught, and backed by you out loud — so staff feel safe stopping a payment even when the request seems to come from the top.

- Put the one-page procedure in writing and post it where bills get paid.
- Set a clear approval amount above which a second person must sign off.
- Tell staff directly: 'I will never be angry about a call-back' — and mean it, so nobody caves to a fake 'urgent' request.
- Make sure a request that looks like it's from you still gets verified — your account or your name can be spoofed.

★ Not sure how to fit this to how you run?

Tell me who pays your bills and how, and I'll help you set up a call-back rule that fits — solo discipline or a written procedure for your team. Call (330) 200-8042.

What it looks like in real life

Three everyday requests, and the calm way to handle each with the rule.

Q: A longtime vendor emails: 'We've changed banks — here are our new payment details for this month's invoice.'

Highest-risk request there is. Don't reply to confirm. Call the vendor at the number from a past invoice or your saved contacts and ask a real person whether their bank details changed. Nine times in ten, they'll say no — it was never them.

Q: An email that looks like it's from the owner: 'I need you to wire \$4,800 today for a deposit — I'm tied up, just get it done.'

Urgency plus secrecy plus a wire. Stop. Reach the owner on a known number — call or text the real phone, don't reply to the email — and confirm face-to-face or voice-to-voice before anything moves.

Q: An invoice arrives that looks just like the usual ones, but the account number at the bottom is different.

Same vendor, new account is a classic tell. Verify by calling the known number before paying, even though everything else looks normal. A matching logo proves nothing — crooks copy those easily.

✓ **The answer is always the same: verify, don't react**

Notice the pattern — in every case the move is identical. You don't have to diagnose the scam. You just run the rule, and the rule does the deciding for you.

If money already went out

If you've just realized a payment went to a crook, don't freeze and don't hide it. Speed matters now.

The hours right after a fraudulent payment are the ones that give you a real chance of getting money back, because banks can sometimes recall or freeze a transfer before it's fully gone. Move quickly and calmly through these steps:

- **Call your bank immediately** — tell them it was fraud and ask them to try to recall or freeze the transfer right now.
- **Report it to the FBI's IC3 at ic3.gov** — their recovery process works best when you report fast, with the details.
- **Keep everything** — the emails, the invoice, the payment confirmation. Don't delete anything.
- **Tell the real vendor or person** who was impersonated, so they can warn others and check their own accounts.
- **Call your insurer** if you carry cyber or crime coverage — see our cyber-insurance guides about social-engineering coverage.

! Report to ic3.gov — and do it quickly

The FBI's Internet Crime Complaint Center at ic3.gov is where to report this kind of wire fraud, and reporting fast gives the best chance of recovery. Don't be embarrassed — these scams fool careful people every day, and reporting helps catch the crooks and sometimes claw money back.

Teaching the rule so it sticks

A rule only works if the people who pay bills actually follow it on a busy Tuesday. Here's how to make it automatic.

Keep the training short and concrete. Walk through one real-looking example together, point out the red flags, and have everyone practice the call-back out loud once. People remember a thing they did far better than a memo they skimmed.

Then make it part of how you do business, not a one-time lecture. Bring it up again when a near-miss happens, praise the person who stopped to verify, and never — ever — punish a false alarm. The moment someone gets scolded for a call-back is the moment the next person stops making them.

✓ Celebrate the call-back, not just the catch

If an employee calls to verify and it turns out the request was genuine, that's a win, not wasted time. Thank them for it, out loud. You're rewarding the habit, and the habit is what saves you on the day it's real.

It cuts both ways: protect your vendors and customers too

You can be the victim — or your name can be the bait used on someone else. A few habits protect both.

Crooks don't only target your payments; they impersonate **you** to fool your customers and vendors. An email that looks like it's from your shop, telling a customer to send their next payment to a 'new account,' can do real harm to people who trust you — and to your reputation.

So set the expectation in both directions. Tell your regular customers and vendors, in plain terms, that your bank details rarely change and that you'll always confirm any change by phone — and you'd like them to do the same. When everyone expects a call-back, the scam loses its footing.

✓ Put your policy in your own emails

A simple line in your invoices and payment emails — 'Our bank details will not change by email; please call us at our known number to verify any change' — quietly trains your customers to resist a fake sent in your name.

Make email itself harder to abuse

The call-back rule is your seatbelt. These settings are the guardrails that keep fakes from getting close.

A lot of this scam depends on getting into a real mailbox or faking one convincingly.

Tightening your email makes both harder, and most of it is free with the email you already have:

- **MFA on every mailbox** so a stolen password alone can't let a crook send mail as you or your staff.
- **External-sender warnings**, if your email system offers them, so a message from outside that poses as an insider is flagged.
- **Review mail rules** now and then — crooks who get in often set a quiet rule to hide their replies.
- **Keep recovery info and admin accounts tight** — see our Microsoft 365 and Google Workspace sign-in guides.
- **Don't reuse passwords** across email and other sites; one leak elsewhere shouldn't open your inbox.

! A hijacked real mailbox is the scary version

When a crook actually logs into a genuine email account — a vendor's, or yours — the fake request comes from the true address, mid-real-thread. Nothing looks off. That's exactly why the call-back to a known phone number is non-negotiable: it's the one check a hijacked inbox can't beat.

Making 'slow down' your default

Every part of this scam fights your instinct to be fast and helpful. The cure is permission to be slow about money.

Busy owners and eager employees are the perfect targets precisely because they want to clear the task and be helpful. The crook borrows that good instinct and aims it at their account. You beat them by deciding, in advance, that money requests are the one place you are always allowed to be slow.

Build small frictions that cost you seconds and cost the scam everything: a fixed rule that payment changes always wait for a call-back, a second approver on bigger amounts, and a culture where 'let me verify that' is normal. None of it slows real business down in any way that matters.

✓ A one-day wait rarely costs you anything real

If a 'vendor' or 'boss' truly can't tolerate a one-day pause to verify a payment, that urgency is itself the warning. Legitimate partners have always been able to wait a day. Scammers never want you to.

The mistakes that let the scam through

Nearly every loss I hear about traces back to one of these. Know them, and you've closed the gaps.

- **Calling the number in the message** to 'verify' — that's the crook's number. Use your own records.
- **Trusting the display name** instead of reading the real address.
- **Letting urgency override the rule** — the rush is the scam, not a reason to skip verifying.
- **Skipping verification for 'small' changes** — a new account number is never small.
- **No second approver** on large or unusual payments.
- **Staying silent after a loss** — every hour of delay lowers your chance of recovery.

! The rule only works if it has no exceptions

A call-back rule you follow 'except when it's really the boss' or 'except when it's urgent' isn't a rule — it's a suggestion, and the scam is built to create exactly those exceptions. Make it apply every time, to everyone, with no special cases.

Set it up this week

You can have this fully in place in an afternoon. Here's the short list.

- ❑ Write the call-back rule in one sentence and decide your second-approver dollar amount.
- ❑ Build your trusted-contacts list — known-good numbers for your top vendors and your bank.
- ❑ Print the one-page procedure and post it where bills get paid.
- ❑ Turn on MFA for every email account — see our sign-in guides.
- ❑ Walk your team (or yourself) through one example out loud and practice the call-back.
- ❑ Add a line to your invoices telling customers your bank details won't change by email.

★ I'll help you stand it all up in one visit

Call-back card, trusted-contacts list, email MFA, a quick practice run with your team — that's a single visit's work, and it protects real money. Call (330) 200-8042.

What a genuine change looks like

Vendors really do change banks sometimes. Here's how to handle a legitimate change without dropping your guard.

The call-back rule doesn't mean payment details can never change — it means every change earns a phone call first. When a real vendor switches banks, your verification simply confirms it: you call the known number, a real person you reach says yes, and you update your records with a note of who you spoke to and when.

Treat a confirmed change like the small, careful event it is. Update your trusted-contacts and payment records in one place, keep the old details until the first new payment clears cleanly, and don't let a genuine change become a habit of trusting email for the next one.

✓ Write down who you verified with

Each time you confirm a change by phone, jot the date, the number you called, and the name of the person who confirmed it. That little note protects you if anything's ever questioned later — and reminds everyone the rule was followed.

Where to report, and where to get free help

If you're hit — or want to get ahead of it — you're not on your own. Here's where to turn.

- **FBI IC3 (ic3.gov):** the place to report BEC, wire fraud, and internet crime. Report fast for the best shot at recovery.
- **Your bank's fraud line:** call the moment you suspect a bad payment — speed is everything.
- **CISA (cisa.gov):** free, plain-English guides and awareness materials for small businesses.
- **CyberOhio and Ohio's free small-business cyber help:** state programs with training and resources — confirm current offerings.
- **Your insurer:** if you carry cyber or crime coverage, call the incident hotline; some losses may be covered.

✓ Reporting helps more than just you

Even if your money can't be recovered, reporting to ic3.gov feeds the bigger picture that helps investigators find patterns, freeze accounts, and warn others. Your report may be the one that helps the next business get their money back.

Common Questions

The questions I hear most about the fake-invoice scam, answered plainly.

Q: Why can't I just reply to the email to confirm the new details?

Because if the email came from a crook, your reply goes right back to them — and they'll happily confirm the fake details. The whole point of the call-back rule is to verify through a different channel, using a phone number from your own records, not from the message.

Q: It really looks like it's from my vendor's real address. Isn't that safe?

Not necessarily. Crooks sometimes break into a real mailbox and send from the genuine address, mid-thread. That's exactly the case the call-back is built for — a phone call to a known number catches it when the email can't be trusted at all.

Q: What dollar amount should trigger a second approver?

Whatever would genuinely hurt to lose — that's a judgment call for your business. Many small shops pick a round number that's rare enough not to slow daily work but low enough to catch the payments a crook would target. And remember: any bank-detail change needs verifying at any amount.

Q: We already got tricked once. Can we get the money back?

Sometimes, if you move fast. Call your bank immediately to try to recall or freeze the transfer, and report to the FBI at ic3.gov right away — recovery works best in the first hours. Keep every email and record, and don't be embarrassed; these scams fool careful people.

Q: Isn't this just common sense? Do I really need a written rule?

The written rule is what holds up on a busy, stressful day when a request feels urgent and official. Common sense bends under pressure; a rule everyone knows and follows doesn't. That's the whole value of writing it down.

★ Got a suspicious payment request right now?

Don't pay it yet — give me a call and we'll walk through the red flags and the call-back together, calmly, before any money moves. Call or text (330) 200-8042.

You don't have to do this alone

You just have to remember that a friendly, patient person is one call away.

I hope this guide made the fake-invoice and payment-redirection scam feel a little less daunting and a lot more doable. Keep it with your other business papers, come back to a page whenever you need it, and don't worry about memorizing anything.

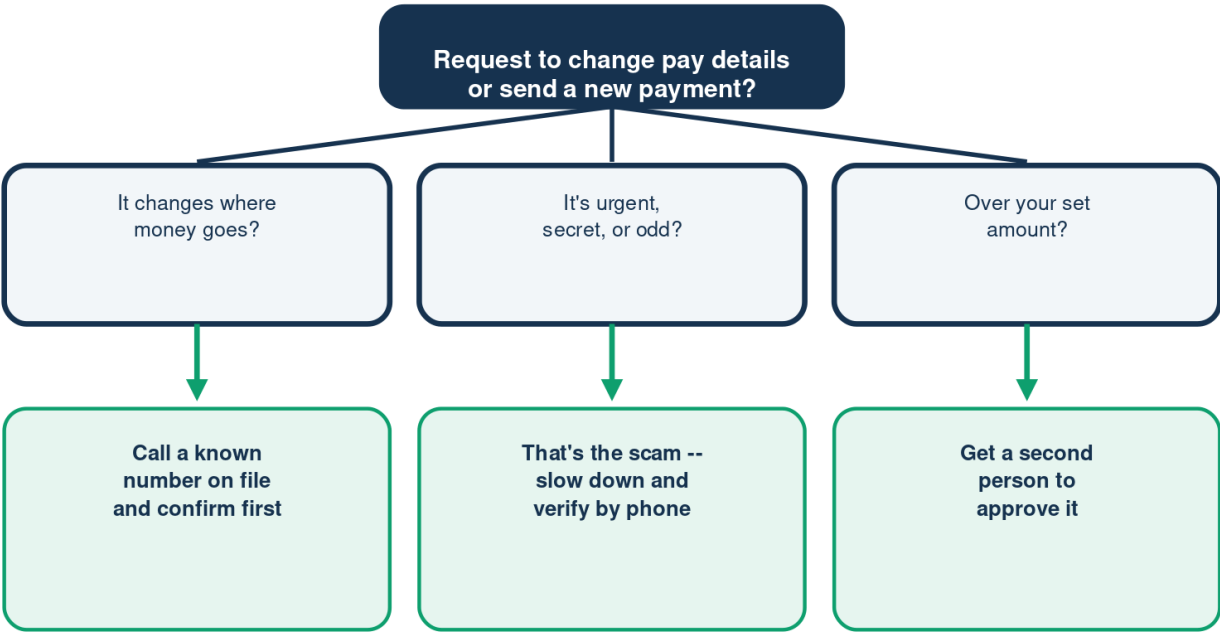
When you'd rather have a hand, that's exactly what I do. I come to your business, work at your pace, and never make you feel rushed or silly for asking. A first visit is a flat \$99, and for the parts that don't need me on-site I can often help right on your screen for \$49. Every visit comes with a 30-day, come-back-free guarantee. I'm a tech helper, not a lawyer or your insurance agent — for the legal and insurance pieces I'll help you understand the questions and line up the right professional.

★ Bill's Home Tech — real help, close to home

Call or text me at (330) 200-8042, or visit BillsHomeTech.com. Serving Atwater and all of Portage County. 30+ years of patient, plain-English tech help — and if you're ever not 100% happy with a visit, I'll make it right or refund it. That's a promise. — Bill

The Call-Back Rule

Run this before any payment change or new wire



Never call the number in the message -- use one from your own records.

Illustration - a schematic, not to scale. Your setup may differ.

Fake Request vs Real One

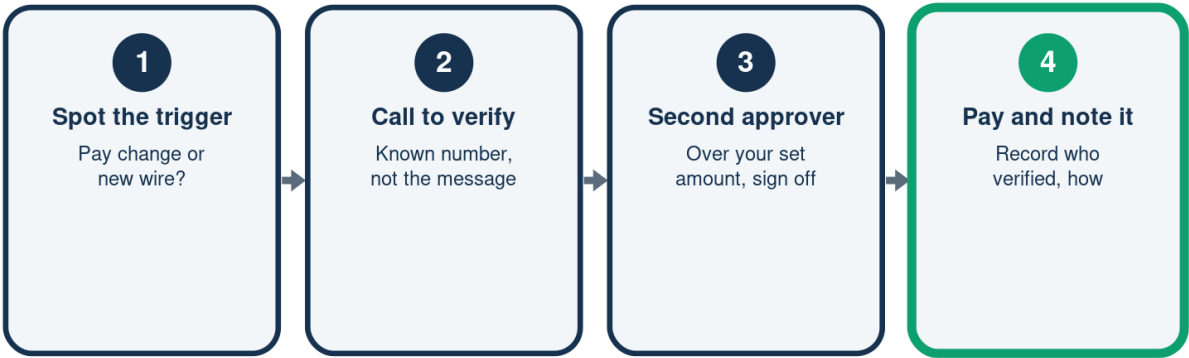
The tells that separate a scam from the real thing

	Scam tends to	Real tends to
Timing	Rush you	Allow a call
Secrecy	Keep it quiet	Fine to check
Account	New, different	Same as always
Verify by	Reply to email	A known phone

Any one scam tell is enough to stop and verify before you pay.

Pay Safely in Four Steps

The habit that beats the scam every time



Something still feels off? Don't pay -- a real partner can wait a day.

If Money Already Went Out

Act fast -- the first hours matter most



Reporting fast to ic3.gov gives the best chance of recovering funds.



Need a Real Person?

You do not have to remember all of it.
You just have to remember you can call.
Friendly, in-person tech help -- I come to you.

BILL'S PROMISE

If you are not 100% happy with a visit, I will make it right -- or refund it. No awkwardness, no fine print. That is how I would want to be treated.

(330) 200-8042 · BillsHomeTech.com

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

— Bill

Prefer help without a visit?

Bill can screen-share and fix many things remotely — a flat \$49, free for Support Plan members.



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 comes from using these guides. Thanks for reading, and stay safe out there.

— *Bill*



Book a visit —
billshometech.com/book

Use of these guides is subject to our Terms of Use (billshometech.com/terms-of-use).

(330) 200-8042 · BillsHomeTech.com

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

For general information only — not professional advice. Use at your own risk. For electrical, gas, water, or ladder work, please call a licensed professional. — Bill's Home Tech