



An Extended Guide · No. 2067

The Cyber-Insurance Application: Answering Every Question Honestly

What the questions mean, and why
an honest answer protects you

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. That same honesty is what this guide is really about: the insurance application asks whether you actually do those things, and your answer has to be true.

Let's fill it out honestly, together

A cyber-insurance application is a page or two of yes-or-no questions about how you run your computers. It looks simple. But each answer is a promise, and a wrong promise can quietly cancel the very protection you're paying for. This guide walks you through it calmly.

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 get comfortable with their technology, in plain language and at a kitchen-table pace. Think of this as me sitting beside you while you fill out the form.

Here's the one idea to carry through every page: answer what is **actually true today**, not what you intend to do, not what you think they want to hear. An honest 'no' keeps your coverage valid. A hopeful 'yes' can hand the insurer a reason to walk away when you need them most.

★ I'll help you answer truthfully — and then make it true

If a question stumps you, that's normal — the wording is often technical. I can look at your setup, tell you what the honest answer is right now, and help you turn a 'no' into a real 'yes' before you sign. Call or text me at (330) 200-8042.

The whole guide, on one page

If you remember only these things, you'll fill out the application the right way.

- ❑ The application is a **sworn statement**. Treat every answer the way you'd treat a signature on a tax return.
- ❑ Answer what is **true today** — not your plans, not your best day.
- ❑ If you're not sure what a question means, find out before you answer. Guessing is how good businesses end up with denied claims.
- ❑ **Multi-factor authentication (MFA)** is the question insurers care about most. 'Mostly' or 'we're working on it' is a 'no.'
- ❑ Keep a copy of the finished application and the proof behind your answers — screenshots, settings, dates.
- ❑ A broker is your ally. Let them help you answer, and read the policy before you buy.

! An overstated answer can void the policy

If you check 'yes, we require MFA everywhere' and it turns out you didn't, an insurer can deny the claim or cancel the policy after a loss — leaving you with both the bill and the premium you already paid. Honesty isn't just right here; it's what makes the coverage real.

Why a form feels like it has teeth

It helps to understand what the insurer is doing when they hand you this application.

An insurer is deciding two things: whether to cover you at all, and what to charge. They can't come inspect your office, so they rely on your answers. In insurance terms, your application becomes part of the contract — a set of representations you're making about your business.

That's why the honesty matters so much. If a loss happens and the insurer discovers an answer wasn't true — that the MFA you promised wasn't actually on, or the backups you described didn't exist — they may argue the contract was based on bad information. Depending on the policy and the facts, that can mean a reduced payout, a denied claim, or a cancelled policy.

None of this is meant to scare you off insurance — it's a genuinely good idea for most small businesses, and our companion guide, 'Do You Need Cyber Insurance?', covers what a policy actually pays for. It's to make sure the policy you buy will be there when you call.

! A quick, important note

This guide explains the idea in plain English so you know what to ask about — it is general information, not legal or insurance advice, and it is not a substitute for reading the actual rule or policy. Laws and requirements change, and your situation may be different, so please confirm the current requirement with a lawyer, your insurance agent, or the agency itself before you rely on it.

Multi-factor authentication: the question they care about most

If there's one line on the form worth getting exactly right, it's this one.

MFA — multi-factor authentication, sometimes called two-step or two-factor sign-in — means a password alone isn't enough to log in. There's a second step: a code from an app, a tap on your phone, or a security key. It's the single most effective thing a small business can do to stop account break-ins, and insurers know it.

The application won't just ask 'do you use MFA?' It usually asks where: on email, on remote access to your systems, on administrator accounts, and on cloud services. The honest answer has to be true for **each** place they ask about. If email has it but your remote-access tool doesn't, the truthful answer about remote access is 'no.'

! 'Mostly on' is a 'no' on this form

Insurers report that MFA is now a baseline requirement — many won't cover a business without it, and denied claims often trace back to MFA that wasn't fully in place. If yours is partial, the honest answer is 'no, not everywhere,' and the smart move is to finish turning it on before you apply. Our Microsoft 365 and Google Workspace guides show you how.

What the common questions are really asking

The wording can be technical. Here's the plain-English translation of the questions you'll see again and again.

The question	What it's really asking
Do you enforce MFA?	Is a second sign-in step required — not just offered — on email, remote access, admin, and cloud?
Do you have endpoint protection / EDR?	Is there antivirus or a monitoring tool on every computer?
Do you keep offline / tested backups?	Could you restore your data if everything were encrypted — and have you actually tried?
Do you patch / update promptly?	Do you install security updates and replace end-of-support software?
Do you train staff on phishing?	Have people been shown how to spot a scam email?
Do you have an incident response plan?	Is there a written who-to-call-and-what-to-do if you get hit?

✓ **Don't answer a question you don't understand**

If a term is fuzzy — 'privileged access management,' 'immutable backups' — that's your cue to ask your broker or me what it means for a business your size. A clear question deserves a true answer, and you can't give one until the question is clear.

Backups and updates: easy to overstate

Two more questions where good businesses accidentally stretch the truth, usually out of optimism.

Backups

The form asks if you keep backups — often whether they're kept 'offline' or somewhere ransomware can't reach, and whether you've tested them. Having a backup running is not the same as knowing it works. If you've never restored from it, the honest answer to 'have you tested your backups?' is 'no.' Our guide 'Can You Actually Restore?' turns that into a 'yes' with a simple quarterly drill.

Updates and end-of-support software

They'll ask whether you apply updates and whether you're still running software that's past its end-of-support date. Windows 10, for example, reached the end of its free security updates in October 2025. Running unsupported software is a common reason for higher premiums or exclusions — and claiming you're current when you're not is a risky answer.

✓ Fix first, then answer

Where you can close a gap quickly — turn on a backup test, update a PC, finish an MFA rollout — do it before you apply. Then your 'yes' is both true and good for your premium.

A truthful 'no' is better than a hopeful 'yes'

It feels backwards, but a few honest no's will serve you far better than a form full of optimistic yeses.

An honest 'no' does two good things. First, it keeps your coverage valid — the insurer priced the risk knowing the real picture, so they can't later say you misled them. Second, it often comes with a roadmap: many insurers will still cover you and simply tell you which controls to add, or give you a window to add them.

A hopeful 'yes,' by contrast, buys you a lower price today and a nasty surprise later. The moment you need the policy most — after a real loss — is exactly when the insurer looks hardest at whether your answers were true.

★ Turn the no's into yeses, at your pace

Most of the gaps I see are fixable in an afternoon or two. Send me the application, and I'll help you sort the honest answers from the ones we can make true before you sign — no judgment, no jargon. Call (330) 200-8042.

Keep the proof behind your answers

If a claim ever happens, you'll be glad you can show your answers were true. A little file now saves a lot of stress later.

For each 'yes' on the application, keep a simple record of how you know it's true: a screenshot of the MFA setting turned on, a note of the date you tested a backup and what you restored, a list of which computers have protection installed. Date everything.

Store this where you can find it — a labeled folder on a backed-up drive or in your cloud account, and ideally a printed copy with your insurance papers. Think of it as the receipts for the promises you made on the form.

✓ A one-page evidence sheet

List each application question you answered 'yes' to, and next to it write where the proof lives. That single page turns a scary audit into a calm five-minute task. Our 'One-Page Security Plan' guide pairs nicely with it.

Lean on your broker — that's what they're for

You don't have to face the application alone, and you shouldn't. A good broker is on your side.

A broker who knows cyber coverage can translate the questions, tell you which answers drive the price, and match you to an insurer that fits a business your size. They can also tell you, honestly, when a 'no' is a dealbreaker and when it's just a note for later.

Ask them to walk you through the policy before you buy, not just the application — what it pays for, the deductible, and especially the exclusions. The next page covers the exclusions worth asking about by name.

! Read it before you sign either document

Both the application and the policy are worth reading slowly. If a broker rushes you past the fine print, that's a reason to slow down, not speed up. There's no silly question to ask about a contract you're signing.

The same form, two very different realities

The form looks the same whether you're one person or twenty, but the honest answers — and the easy wins — depend a lot on how your business runs.

If you're a solo operator or a tiny shop

With one or a few people, your 'systems' are probably your email, a couple of laptops, and a cloud account or two. That's good news: you can often make every answer a true 'yes' in a single afternoon.

- Turn on MFA for your email and cloud accounts first — it covers most of the form's biggest questions.
- One tested backup of your important files can answer the backup questions honestly.
- You likely have no 'remote access' or 'admin' sprawl to worry about — answer those plainly.
- Keep your handful of devices updated; it's a quick, honest 'yes.'

If you have employees and handle customer data

More people means more accounts, more devices, and more honest no's to track down before you can answer. It also means the questions about offboarding, training, and admin accounts actually apply to you.

- MFA must be on for **everyone**, including the owner and any admin accounts — see our Microsoft 365 and Google Workspace guides.
- You'll need a real answer on staff training and on cutting off access when someone leaves (we have guides for both).
- Separate everyday accounts from administrator accounts before you answer the 'privileged access' questions.
- If you take cards or prepare taxes, extra rules may apply — see the PCI and FTC Safeguards guides.

★ Not sure which answers are honest for your setup?

Tell me how your business runs — how many people, what you use for email and files — and I'll help you figure out the true answer to each question and which gaps are worth closing first. Call (330) 200-8042.

The exclusions worth asking about

An exclusion is something the policy won't pay for. Knowing them before you buy prevents the worst kind of surprise.

Every policy has them, and they vary. You don't need to memorize the list — you need to ask your broker which ones are in **your** policy and what they mean for a business like yours.

These are the ones that trip up small businesses most often:

- **Missing-control exclusions:** if you promised a control like MFA or prompt patching and it wasn't actually in place, the related loss may not be covered.
- **Known or prior incidents:** a problem you were already aware of before the policy started.
- **Acts of war / nation-state attacks:** a contested area — ask how your policy defines it.
- **Hardware replacement and lost future profits:** often not covered; the policy pays to respond and recover, not to upgrade.
- **Intentional insider acts:** deliberate wrongdoing by your own people.

✓ Turn exclusions into a checklist

Each exclusion is really a hint about what to shore up. 'Won't pay if MFA was off' is the insurer telling you, plainly, to turn MFA on. Treat the exclusions page as free security advice.

What you're actually buying

Cyber coverage comes in two broad halves. Knowing the difference helps you answer the application and judge the quote.

First-party coverage — your own costs

This pays for what your business absorbs directly: the investigation (forensics) to find out what happened, restoring your data and systems, lost income while you're down, and — depending on the policy — ransom or extortion costs and the price of notifying affected customers.

Third-party coverage — claims from others

This pays when someone else is harmed because their data was exposed through you: lawsuits, legal defense, settlements, and certain regulatory costs. If you hold customer or patient information, this side matters.

Our companion guide, 'Do You Need Cyber Insurance?', digs into both in plain English. For the application, just know which side of coverage you're most worried about, and ask the broker to confirm the quote includes it.

✓ Match the coverage to your real risk

A shop that holds lots of customer records leans on third-party coverage; a shop that would simply be shut down by an outage leans on first-party. Most need some of both — say so on the form and to your broker.

Gather these before you open the form

Half the stress of the application is hunting for answers mid-form. A few minutes of prep makes it calm.

- ❑ A list of the services you sign into: email, cloud files, accounting, point-of-sale, any remote-access tool.
- ❑ Which of those have MFA turned on — check each one, don't assume.
- ❑ How many employees have logins, and who has administrator rights.
- ❑ What you back up, where it's stored, and the last time you tested a restore.
- ❑ Whether any computers run end-of-support software (like Windows 10 without extended updates).
- ❑ Roughly how many customer records you hold, and whether you take credit cards.

★ I can help you build this list fast

In one visit I can walk your office, check each sign-in for MFA, and write down the honest state of things so the application takes minutes, not a weekend. Call (330) 200-8042.

The form comes back every year

A cyber policy isn't set-and-forget. Each renewal asks again — and the questions tend to get tougher.

Insurers raise the bar as threats change. A control that was optional when you first signed up may be required at renewal, and the honest answer has to keep up. Treat renewal as a yearly check-up: re-verify each 'yes' is still true, and close any gaps the new questions reveal.

This is also when overstated answers come home to roost. If you stretched the truth last year and nothing happened, it's tempting to do it again — but each year you do, you're betting your coverage on not having a claim. Far better to use the renewal to actually finish the work.

✓ Put the renewal on your calendar — with a head start

Mark a reminder a month before your policy renews. That month is enough to re-test a backup, confirm MFA is still on for everyone, and answer the new questions truthfully instead of in a panic.

The mistakes that bite later

Almost every denied small-business claim I read about traces back to one of these. Now you'll know them in advance.

- **Checking 'yes' to MFA** when it's only on some accounts. This is the number-one costly answer.
- **Describing backups you've never tested** as if you know they work.
- **Letting a manager or vendor fill out the form** without confirming each answer is actually true.
- **Guessing at a question's meaning** instead of asking.
- **Not updating answers at renewal** after your setup changed.
- **Throwing away the application** — keep a copy and the proof behind it.

! The form is not the place to be optimistic

Optimism is a fine way to run a business and a dangerous way to fill out an insurance application. Save the optimism for your goals; keep the form strictly factual.

What an honest answer looks like

To make it concrete, here's how a careful owner might handle three tricky lines — without overstating anything.

Q: 'Do you require multi-factor authentication for all email access?'

Honest answer if email MFA is on for everyone: 'Yes.' If the owner has it but two staff don't yet: 'No' — and the fix is to enroll those two before applying, then answer 'yes.'

Q: 'Are backups stored offline or otherwise isolated, and tested?'

If backups run to the cloud but have never been restored: 'We keep backups but have not tested a restore.' Then run one test (a file, a mailbox) and you can truthfully say they're tested.

Q: 'Do you operate any end-of-support software?'

If a back-office PC still runs Windows 10 without extended updates: 'Yes, one machine' — and note your plan to update it. Don't hide it; it's a common, fixable finding.

✓ Honest and specific beats vague

Where the form gives you room to explain, a short, specific note ('MFA on all accounts except two new hires, enrolling this week') reads far better to an underwriter than a bare box left ambiguous.

What if you can't honestly say yes yet?

Finding gaps while filling out the form isn't failure — it's the form doing its job. Here's the calm path forward.

If several answers would have to be 'no' today, you have two good options, and neither involves lying. You can apply honestly now and take the terms offered — many insurers will still cover you and give you time to add controls. Or you can spend a short while closing the biggest gaps first, then apply from a stronger, cheaper position.

The gaps worth closing first are almost always the same: MFA everywhere, one tested backup, updates current, and admin accounts separated from everyday ones. Those four answers carry most of the weight on the form and do the most to actually protect you.

★ Let's close the big gaps first

I can knock out MFA, a backup test, and updates in a visit or two, so your application goes from a wall of no's to a confident set of yeses. No pressure, no upsell — just the work. Call (330) 200-8042.

Once the policy is in force

Buying the policy is step one. A few small habits keep it valid and make it useful if you ever need it.

Keep doing the things you promised — MFA stays on, backups keep getting tested, updates keep happening. If your setup changes in a big way (new remote-access tool, a new location, you start taking cards), tell your broker; a material change can affect coverage.

And find the policy's incident hotline **now**, while nothing is wrong. Most cyber policies want you to call them first after an incident, because they direct the response and bring in the forensics and legal help. Our guide 'The First Hour After a Hack' explains why that call comes before almost anything else.

✓ Tape the hotline number inside a drawer

The worst time to go hunting for your policy number is during an actual emergency. Write the insurer's incident hotline and your policy number somewhere everyone can find it — and somewhere that doesn't rely on the computers that might be down.

Who should fill it out and sign it

Because the application is a sworn statement, it matters who's behind each answer.

The person who signs is vouching for the whole form, so the owner or a trusted manager should own it — not hand it off blindly to a vendor or a part-time helper. It's perfectly fine to get technical answers from your IT person or from me; just confirm each one yourself before you sign.

If an outside IT provider helps, ask them to show you the setting, not just assure you it's done. 'Here's the screen showing MFA is enforced' is worth far more than 'yes, that's all set.' Our guide on hiring outside IT help covers what to keep control of.

! Your signature, your responsibility

Even when someone else fills in the boxes, the signature makes the answers yours. Read the finished form top to bottom before you sign, and don't sign a box you can't personally stand behind.

A simple system you can reuse every year

Make the application easy forever by keeping three small things up to date.

- ❑ A one-page list of every account and whether MFA is on — update it whenever you add a service or a person.
- ❑ A backup log: what you back up and the date of your last tested restore.
- ❑ An evidence folder with dated screenshots proving your 'yes' answers.

With those three in a labeled folder, next year's renewal is a half-hour job instead of a scramble, and you'll always be able to prove your answers were true. It's the same tidy habit behind our 'One-Page Security Plan' guide.

✓ Small and current beats big and stale

Don't build a giant binder you'll never touch. Three living pages you actually keep current are worth more than a thick policy manual gathering dust on a shelf.

Common Questions

The questions I hear most from owners facing a cyber-insurance application, answered plainly.

Q: What happens if I answer something wrong by accident?

Tell your broker as soon as you realize. An honest correction is far better than an error that surfaces during a claim. Insurers deal with corrections all the time; it's deliberate misstatements that cause trouble.

Q: Will a bunch of 'no' answers mean I can't get covered?

Usually not. Many insurers will still cover a small business and simply price it accordingly or ask you to add controls. An honest 'no' keeps the door open; a false 'yes' can slam it shut later.

Q: Is MFA really that big a deal on the form?

Yes. It's the control insurers weigh most heavily, and partial MFA is a common reason claims get denied. If you do one thing before applying, make it finishing your MFA rollout.

Q: Can you just fill it out for me?

I can help you find the honest answer to every question and fix the gaps — but you (or your manager) should review and sign it, because it's your sworn statement. I'm your guide, not your signature.

★ Staring at an application right now?

Send it my way or give me a call, and we'll go through it line by line together — honestly, calmly, and in plain English. 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 your cyber-insurance application 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

Answer What's True Today

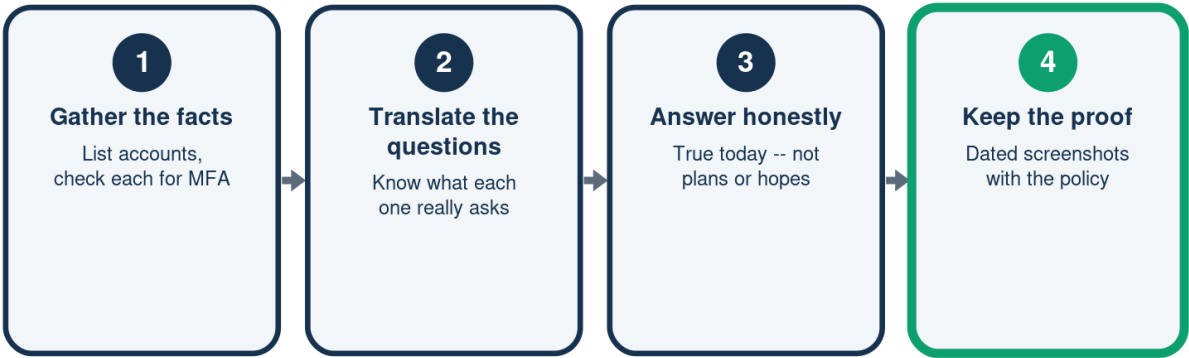
The honest answer protects your coverage

	Your real situation	The honest answer
MFA on all accounts	Everyone, every app	Yes
MFA on some	Owner yes, staff no	No -- fix first
Backup never tested	It runs, untested	Not tested yet
Old Windows PC	Past end-of-support	Yes, disclose it

A truthful 'no' keeps coverage valid; a hopeful 'yes' can void it.

Filling It Out in Four Steps

The calm way through the application



Close easy gaps before you answer, then your 'yes' is true and cheaper.

The Two Halves of Cyber Coverage

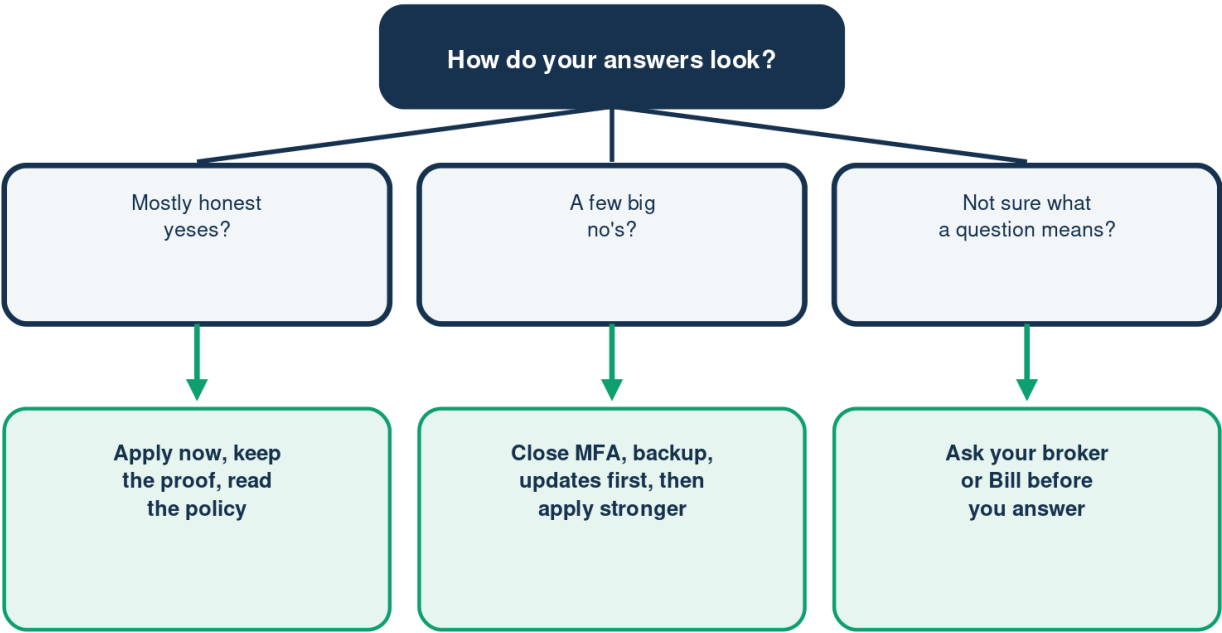
What you're actually buying

	Covers	Pays for
First-party	Your own costs	Recovery, downtime
Third-party	Harm to others	Lawsuits, defense
Ransom/extortion	Often first-party	If your policy adds it
Notification	Telling customers	Varies by policy

Most small businesses need some of both -- ask your broker to confirm.

Ready to Apply, or Fix First?

Let your honest answers point the way



Never guess an answer -- a wrong 'yes' can cost you the whole claim.

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



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