



An Extended Guide · No. 2068

Do You Need Cyber Insurance? What a Small Policy Covers and Costs

What it pays for, what it
won't, and how to compare quotes

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. Cyber insurance sits behind those habits as a safety net — it does not replace them, and this guide helps you decide whether it is worth buying for a business like yours.

Let's figure out if a policy is worth it for you

Cyber insurance is coverage for the costs of a hack, a ransomware attack, or a data breach — the cleanup, the lost income, and the people you may have to notify. The question most owners ask me is simple: do I really need it, and what would it even cost? Let's work through that 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. I don't sell insurance and I earn no commission — this is just honest advice to help you ask a broker the right questions.

Here's the short version up front: for most small businesses that rely on computers, email, or customer records, some cyber coverage is a sensible idea. But the right amount — and the price — depends entirely on how your business runs. We'll sort that out together.

★ I'll help you understand the choice, not sell you one

I can look at how your business actually uses technology and help you figure out what a policy would need to cover — then you take that to a broker. No pressure, no commission, just plain talk. Call or text me at (330) 200-8042.

The whole guide, on one page

If you remember only these things, you'll make a smart decision about cyber insurance.

- ❑ Cyber coverage comes in two halves: **first-party** (your own costs) and **third-party** (claims from others whose data was exposed).
- ❑ Premiums **vary widely** and depend heavily on your size, your data, and your security controls — there's no one price, so get quotes.
- ❑ Good controls lower your price. **MFA is now a baseline** most carriers expect, and many won't quote you without it.
- ❑ Every policy has **exclusions** — things it won't pay for. Read them before you buy, not after a loss.
- ❑ Compare quotes **apples to apples**: same limits, same deductible, same coverages — the cheapest number isn't always the best policy.
- ❑ The application is a sworn statement — answer honestly. See our cyber-insurance application guide.

✓ There's no silly question to ask a broker

Insurance language is dense on purpose. If a term on the quote is fuzzy, that's your cue to ask your broker to explain it in plain English before you sign. A policy you understand is worth more than a cheaper one you don't.

What cyber insurance actually is

Before you can decide if you need it, it helps to know what you'd be buying.

Think of cyber insurance the way you think of your other business policies. General liability covers a slip-and-fall; property insurance covers a fire. Cyber insurance covers the mess that follows a hack, a ransomware lockup, or a leak of the personal information you hold — the costs that a regular business policy usually won't touch.

It's not a security tool, and it won't stop an attack. It's a financial backstop for the day something gets through, plus — and this is the part owners underrate — a team of experts the insurer brings in to help you recover. For a small business, that expert help can matter as much as the money.

! A quick, important note

This guide explains cyber insurance in plain English so you know what to ask about — it is general information, not insurance advice, and it is not a substitute for reading the actual policy. Coverage terms, conditions, and prices vary by carrier and change over time, and your situation may be different, so please confirm the specifics with a licensed insurance agent or broker before you rely on anything here.

First-party coverage: your own costs

This is the half that pays for what your business absorbs directly when something goes wrong.

First-party coverage is the money that comes to you to put your own business back together. When people picture cyber insurance, this is usually what they're imagining. Depending on the policy, it can include:

- **Incident response and forensics** — the experts who figure out what happened and how to stop it.
- **Data and system restoration** — the work to rebuild or recover what was damaged or encrypted.
- **Business interruption** — income you lose while you're shut down or working at half speed.
- **Extortion and ransom costs** — often included, sometimes as an add-on; confirm it's there.
- **Breach notification** — the cost of telling affected customers and any required agencies.

✓ For many small shops, this is the half that saves you

If a ransomware attack would simply shut you down, first-party coverage — especially business interruption and restoration — is probably what you care about most. Say so when you talk to a broker.

Third-party coverage: claims from others

This is the half that pays when someone else is harmed because their information was exposed through you.

If you hold personal information about customers, patients, donors, or employees — names with Social Security numbers, card numbers, health details — then a breach doesn't just hurt you. It can harm the people whose data leaked, and they (or a regulator) may come looking for someone to answer for it.

Third-party coverage is built for that. Depending on the policy, it can pay for legal defense, settlements or judgments, and certain regulatory costs tied to a breach of other people's data. The more sensitive records you hold, the more this side matters.

! Holding customer data raises the stakes

A plumber with three vans and a church office can both get hacked, but the one holding a long list of customers' card numbers or members' personal details has far more third-party exposure. If that's you, don't skip this half — our Ohio breach-notification guide explains why.

The two halves, side by side

Most small businesses need some of both. Here's the plain-English difference so you can judge a quote.

Question	First-party	Third-party
Whose costs?	Yours	Someone else's
Typical trigger	You're hacked or down	Others' data leaked
Pays for	Recovery, lost income	Lawsuits, defense
Matters most if	An outage would hurt	You hold lots of data

When you read a quote, find both halves and check the dollar limits on each. A policy heavy on one side and thin on the other may not match your real risk. Our cyber-insurance application guide covers how the questions you answer tie back to these coverages.

✓ **Name your worst day out loud**

Ask yourself: what would actually hurt most — being shut down for a week, or a leak of customer records? Your answer tells you which half to weigh more heavily, and gives your broker a clear starting point.

What a policy won't pay for

An exclusion is something the policy specifically doesn't cover. Knowing them before you buy prevents the worst kind of surprise.

You don't need to memorize the list — you need to ask your broker which exclusions 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 losses:** if you promised a control like MFA and it wasn't actually on, 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 or 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.

! The exclusions page is free security advice

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. Read the exclusions slowly — they tell you how the policy really behaves.

What does a small policy cost?

The honest answer is the one owners least want to hear: it depends — a lot.

There's no single price for cyber insurance, and anyone who quotes you a firm number without knowing your business is guessing. The premium depends on your size, your revenue, the kind and amount of data you hold, the coverage limits and deductible you pick, and — heavily — the security controls you have in place.

That's actually good news. Because controls move the price, the things that make you safer also tend to make you cheaper to insure. The same afternoon's work that turns on MFA and tests a backup can lower your quote. We'll look at those controls on the next page.

✓ Get quotes — more than one

The only way to know your real cost is to get quotes for your actual business, from more than one carrier, and compare them. Prices and appetites differ widely between insurers, so one 'no thanks' or one high number doesn't mean coverage is out of reach.

The controls that lower your premium

Insurers price the risk they see. Show them a well-run shop and the number tends to come down.

Carriers have learned which habits actually prevent claims, and they reward them. These are the controls that most often move a quote in your favor — and, not by accident, they're the same ones that protect you:

- ❑ **MFA everywhere** — on email, remote access, admin accounts, and cloud. This is the big one; many carriers require it.
- ❑ **Tested backups** — kept where ransomware can't reach them, and actually restored at least once.
- ❑ **Updates kept current** — no end-of-support software quietly running past its last security update.
- ❑ **Endpoint protection** on every computer, kept turned on and up to date.
- ❑ **Staff who can spot a scam email** — a little training goes a long way with underwriters.

★ Let's turn on the cheap wins first

Most of these I can set up with you in a visit or two — MFA, a backup test, updates. Do them before you apply and your quote reflects the safer, cheaper business you've become. Call (330) 200-8042.

Two businesses, two very different needs

Whether you need a policy — and which half of coverage matters most — depends a lot on how your business runs and what you hold.

If you're a solo operator or a very small shop

With one or a few people and little customer data on hand, your biggest risk is usually being knocked offline — email down, files locked, no way to work. First-party coverage tends to matter most to you.

- Lean toward coverage that gets you running again: restoration and business interruption.
- You may hold less personal data, so your third-party exposure can be smaller — but confirm what you actually keep.
- A smaller policy with solid controls can be surprisingly affordable; get a quote before assuming it's out of reach.
- Keep it simple — one carrier, clear limits, a deductible you could actually cover.

If you have employees and hold customer or member data

More people and more records mean more ways to get hit and more people who could be harmed if data leaks. Both halves of coverage matter, and the third-party side grows with the sensitivity of what you keep.

- Weigh third-party coverage seriously if you hold Social Security numbers, card data, health, or donor details.
- Expect the application to ask about staff training and cutting off access when someone leaves — our guides cover both.
- Breach-notification costs can be real; make sure that coverage is there — see our Ohio breach-notification guide.
- If you prepare taxes or arrange financing, extra rules apply — see our FTC Safeguards and tax-preparer plan guides.

★ Not sure how much coverage your setup calls for?

Tell me how your business runs — how many people, what data you keep, what would hurt most if you got hit — and I'll help you frame it so your broker can quote the right policy. Call (330) 200-8042.

So — do you actually need it?

Here's a plain way to decide, without a sales pitch.

Cyber insurance makes the most sense when a cyber incident could do real financial damage you couldn't easily absorb. For most small businesses that run on email and computers, that bar is lower than owners think. Ask yourself these questions honestly:

- If my systems were locked for a week, could I still pay my bills and my people?
- Do I hold personal information about customers, members, or employees that could leak?
- Would I know who to call and how to pay for the cleanup if I got hit tomorrow?
- Does a contract, lender, or client already require me to carry cyber coverage?

If you answered 'that would really hurt' or 'I'm not sure' to any of these, a policy is worth pricing out. Insurance is for the losses you couldn't comfortably write a check to cover yourself.

✓ It's a judgment call, not a mandate

For most businesses cyber insurance is voluntary — but a few contracts and lenders now require it. Check your existing agreements before you decide; the choice may already be partly made for you.

Comparing quotes apples to apples

The cheapest number on the page isn't automatically the best deal. Here's how to compare fairly.

Two quotes can look wildly different and still be for the same business — because they cover different things. Before you compare prices, make sure you're comparing the same policy. Line up these pieces side by side:

Compare this	Why it matters
Coverage limit	The most the policy will pay — a low limit, low price isn't a bargain.
Deductible	What you pay before coverage kicks in — higher deductible, lower premium.
First vs third-party	Make sure both halves you need are actually included.
Sub-limits	Caps hidden inside coverage — ransom or notification may be limited.
Exclusions	What's carved out — a cheap policy may simply cover less.

✓ **Ask the broker to normalize the quotes**

A good broker will happily re-quote two carriers at the same limit and deductible so you're comparing like for like. If the numbers still differ, now you're seeing a real difference, not an apples-to-oranges trick.

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

You don't have to navigate this alone, and you shouldn't. A good broker or agent is on your side.

An independent broker who knows cyber coverage can shop several carriers for you, translate the quotes, and match you to an insurer whose appetite fits a business your size. They can also tell you, honestly, when a coverage is essential and when it's a nice-to-have you can skip to save money.

Come prepared and the conversation goes faster: know roughly how many people have logins, what data you hold, and which security controls you already have. That's the same homework our cyber-insurance application guide walks you through.

! Read the policy, not just the quote

A quote is a summary; the policy is the contract. Ask to see the actual coverage terms and exclusions before you buy, and if anyone rushes you past the fine print, that's a reason to slow down, not speed up.

The application is part of the deal

Buying coverage starts with answering questions truthfully — and those answers become part of the contract.

To quote you, a carrier hands you an application: a page or two of questions about how you run your computers. Each answer is a promise. If a loss happens and the insurer finds an answer wasn't true — the MFA you claimed wasn't really on — they can reduce the payout, deny the claim, or cancel the policy.

So the rule is simple: answer what is **actually true today**, not what you intend to do. An honest 'no' keeps your coverage valid; a hopeful 'yes' can quietly void it. Our companion guide, the cyber-insurance application guide, walks through every question line by line.

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

If a question stumps you, I can look at your setup, tell you the honest answer right now, and help turn a 'no' into a real 'yes' before you sign. Call (330) 200-8042.

Limits, deductibles, and sub-limits

Three numbers decide how much protection you're really buying. Here's what each one means.

The limit

This is the most the policy will pay in total. Pick it based on what a bad incident could realistically cost you — recovery, lost income, notification, legal help — not just the smallest number that fits your budget. A limit that's too low can leave you exposed exactly when it counts.

The deductible

This is what you pay out of pocket before coverage kicks in. A higher deductible lowers your premium — but only choose one you could actually cover in a pinch.

Sub-limits

These are smaller caps hidden inside the main limit — for example, a separate, lower ceiling on ransom payments or notification costs. A policy can look generous overall while quietly capping the coverage you'd lean on most, so ask your broker to point out every sub-limit.

Coverages worth asking about by name

Some protections aren't always in the base policy. Ask about these specifically so nothing you need gets left out.

- **Business interruption:** lost income while you're down — often the coverage a small shop needs most.
- **Ransomware and extortion:** confirm it's included and check the sub-limit; it's sometimes separate.
- **Social-engineering / fraudulent-transfer coverage:** for money lost to a fake-invoice or 'new bank details' scam — often excluded or limited, so ask. See our fake-invoice call-back guide.
- **Breach notification and credit monitoring:** the cost of telling affected people and helping protect them.
- **Dependent / vendor outage:** losses when a cloud provider or key vendor you rely on goes down.

! Scam-transfer losses may not be where you think

Money wired to a crook after a convincing 'new bank details' email is a common, painful loss — and it's often not covered unless you specifically add social-engineering coverage. Ask your broker in plain terms: 'If my bookkeeper gets tricked into wiring money, does this pay?'

Reading the policy before you buy

You don't have to understand every line — you do have to find a handful of key parts and ask about them.

When the full policy lands, don't let its length scare you off. You're looking for just a few things, and a highlighter plus your broker on the phone will get you through it in half an hour:

- ❑ The **declarations page** — your limits, deductible, and what coverages you actually bought.
- ❑ The **exclusions** — what the policy won't pay for.
- ❑ Any **conditions or warranties** — controls you must keep in place (like MFA) for coverage to hold.
- ❑ The **sub-limits** — smaller caps inside the big one.
- ❑ The **incident reporting rules** — how fast and how you must report a loss, and the hotline to call first.

✓ Find the incident hotline now, while nothing's 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 team. Write that hotline and your policy number somewhere everyone can find it — including somewhere off the computers that might be down.

The policy comes up every year

Cyber insurance isn't set-and-forget. Each renewal is a chance to re-shop and re-check.

Insurers raise the bar as threats change, so a control that was optional when you first signed up may be expected at renewal. Treat renewal as a yearly check-up: confirm the controls you promised are still on, update anything that changed in your business, and answer the new application questions honestly.

It's also a good moment to get fresh quotes. Your price can move as your controls improve or as the market shifts, and a broker shopping your renewal may find a better fit. Don't assume this year's carrier is automatically next year's best deal.

✓ Put the renewal on your calendar — early

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 scramble.

The mistakes that cost owners later

A few predictable missteps turn a good policy into a nasty surprise. Now you'll know them in advance.

- **Buying on price alone** — the cheapest quote often simply covers less. Compare coverage first.
- **Overstating your controls** on the application — a false 'yes' can void the very coverage you're paying for.
- **Ignoring sub-limits** — discovering the ransom or notification cap was tiny only after a loss.
- **Skipping social-engineering coverage** and assuming wire-fraud losses are covered when they're not.
- **Letting the policy lapse** or changing your setup without telling the broker.
- **Treating insurance as a substitute for security** — it pays for the mess; it doesn't prevent it.

! Insurance is the backstop, not the defense

A policy is no reason to skip MFA, backups, and updates — in fact those are usually required for coverage to hold. Buy the policy and do the basics; each makes the other work.

A simple plan for buying the right policy

Pull it all together into a short, do-this-week list.

- ❑ Write down your worst day — being shut down, a data leak, or both — so you know which coverage to weigh.
- ❑ Turn on the cheap wins first: MFA everywhere, a tested backup, updates current. They lower your price and your risk.
- ❑ List what you sign into and what data you hold — the same prep as the application guide.
- ❑ Call an independent broker and ask for quotes from more than one carrier, at matching limits and deductibles.
- ❑ Read the declarations, exclusions, sub-limits, and conditions — ask the broker about anything unclear.
- ❑ Save the policy, the application, and the incident hotline somewhere everyone can find them.

★ Want a hand getting ready to shop?

I can help you do the security homework and frame your real risk so your broker can quote the right policy — no commission, no pressure, just honest prep. Call (330) 200-8042.

Common Questions

The questions I hear most from owners weighing cyber insurance, answered plainly.

Q: How much does cyber insurance cost for a small business?

There's no single answer — it varies widely with your size, data, coverage limits, deductible, and especially your security controls. The only way to know is to get quotes for your actual business and compare them. Good controls like MFA tend to lower the price.

Q: Do I really need it if I'm just a one-person shop?

Maybe — it depends on what a cyber incident would cost you. If being locked out for a week would really hurt, or you hold customer data that could leak, it's worth pricing out. For many small shops a modest policy is more affordable than they expect.

Q: Isn't my regular business insurance enough?

Usually not. General liability and property policies typically don't cover a hack, ransomware, or a data breach, and some now specifically exclude them. Ask your agent what your current policies actually say about cyber losses.

Q: Will having MFA and backups really lower my premium?

Often, yes — and sometimes it's the difference between getting a quote and being declined. Carriers price the risk they see, and strong controls make you cheaper to insure. Turn them on before you apply.

Q: What's the difference between first-party and third-party coverage?

First-party pays your own costs — recovery, lost income, notification. Third-party pays claims from others whose data was exposed through you — lawsuits, defense, settlements. Most small businesses need some of both.

★ Weighing a policy right now?

Give me a call and we'll talk through what your business actually needs covered, in plain English, before you sit down with a broker. No commission, no pressure. 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 question of cyber insurance 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 Two Halves of Cyber Coverage

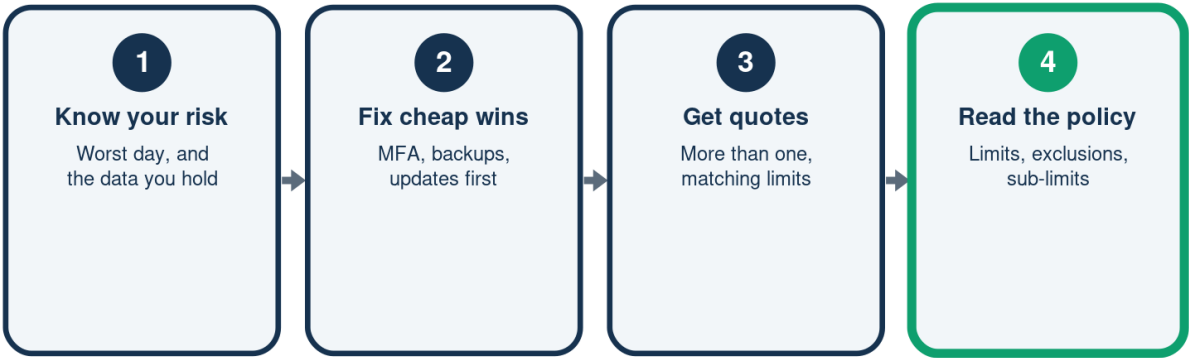
Most small businesses need some of both

	First-party	Third-party
Whose costs	Yours	Others'
Trigger	You're hit	Their data leaks
Pays for	Recovery, income	Lawsuits, defense
Weigh if	Outage would hurt	You hold data

Name your worst day -- outage or data leak -- to see which half matters most.

Shopping Smart in Four Steps

The calm way to buy the right policy



Better controls lower the price, so do the easy security work first.

What Moves Your Premium

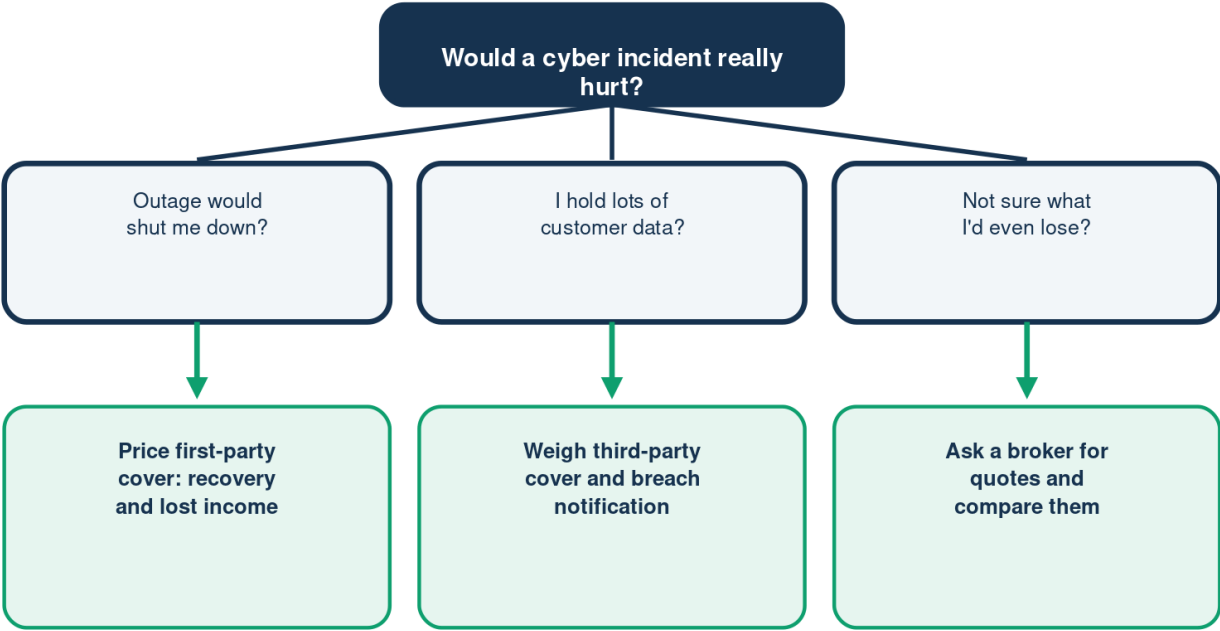
Controls and choices that raise or lower the price

	Lowers price	Raises price
Sign-in	MFA everywhere	No MFA
Backups	Tested, offline	None or untested
Software	Updated	Past end-of-support
Deductible	Higher you pay	Very low

The habits that make you safer also tend to make you cheaper to insure.

Do You Need a Policy?

A plain way to decide, without a sales pitch



Insurance is for losses you couldn't comfortably cover out of pocket.

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