



An Extended Guide · No. 1909

The Card-Security Questionnaire — What the Smallest Merchants Must Do

PCI and the SAQ in plain English
— doable without a consultant

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

★ This is far more doable than it sounds

The words 'PCI compliance' make a lot of owners' eyes glaze over, and I understand why — it sounds like something you'd need to hire a consultant for. For most small shops, you don't. If you take cards through Square, Clover, Toast, or Shopify on their own hardware, you're already doing most of the work. This guide shows you the short form and how to fill it in.

Let's demystify the card-security questionnaire

Every business that takes cards agrees to follow a card-security standard. Once a year, most small merchants confirm they're following it by answering a questionnaire. That's really all this is.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. In 30+ years of helping folks with their technology, I've watched this one scare more small-business owners than it ever needed to. It has a serious name and a serious purpose, but the paperwork for a typical small shop is short and plain once someone walks you through it.

I'll be straight with you: I run my own little business on Square, so I know that path best, but the same ideas apply whichever system you use. I'm a tech helper, not your payment processor and not a security auditor — so for the exact form that applies to you, your processor has the final word, and I'll tell you how to ask them.

✓ You don't have to memorize any of this

Read it once so the words stop being scary, then keep the guide handy for when your processor emails about your yearly questionnaire. That's the only time most owners ever think about it.

The whole thing, on one page

If you remember only these, you'll handle this fine without paying anyone to do it for you.

- ❑ PCI DSS is the card-security standard every business that takes cards agrees to follow. The current version is v4.0.1 (as of late 2026).
- ❑ Small merchants confirm they follow it with a short Self-Assessment Questionnaire (SAQ), and sometimes a network scan.
- ❑ Which SAQ you use depends on HOW you take cards — not on how big you are.
- ❑ Using Square, Clover, Toast, or Shopify with their own listed hardware does most of the heavy lifting for you.
- ❑ Your part: strong unique passwords, turn on multi-factor authentication, and NEVER write down or store full card numbers yourself.
- ❑ There may be a PCI fee, and a non-compliance penalty fee if you skip it — so it's worth doing.
- ❑ Confirm YOUR exact SAQ type with your processor before you fill anything in.

✓ One rule to hold onto

The less card data that ever touches your own equipment or your own hands, the shorter your questionnaire. Let your POS system handle the cards, and keep your part small on purpose.

What PCI DSS actually is

Let's put the name in plain English before we go any further.

PCI DSS stands for the Payment Card Industry Data Security Standard. It's a set of security rules written by the card networks to keep cardholder data safe. Every business that accepts cards agrees to follow it — it's part of the deal when you sign up to take payments.

The current version is **v4.0.1**, and that's what all 2026 assessments use (confirm current with your processor). A batch of future-dated requirements in that version has been in force since March 31, 2025, so by now they simply apply. The good news: for a small shop using a modern POS system, your provider shoulders most of those requirements.

The standard isn't a law passed by a legislature — it's a rule the card networks enforce through your processor. But treat it as mandatory, because your right to take cards depends on it.

★ Why it exists, in one breath

Every rule in here boils down to one idea: don't let a customer's card number leak. When you see it that way, the questionnaire stops feeling like bureaucracy and starts feeling like common sense.

The Self-Assessment Questionnaire — your yearly check

Big companies hire outside auditors. The smallest merchants get to self-assess with a short questionnaire — hence the name.

A Self-Assessment Questionnaire, or SAQ, is a list of yes/no security questions you answer once a year to confirm you're following the standard. You sign it and keep it (and usually submit it through your processor's portal). Some setups also need a quarterly network scan from an approved vendor — your processor will tell you if yours does.

Here's the part that saves you: there isn't one giant questionnaire. There are several short ones, and which one you use depends entirely on HOW you take cards. The more you outsource to your POS system, the shorter your SAQ.

✓ Self-assessment means you can do it

The word 'self' is the whole point. For most small shops this is a form you can read, understand, and sign yourself — not something that requires a paid consultant. Slow down, read each question, and ask your processor if one isn't clear.

The common SAQ types, in plain English

Don't try to memorize these. Skim them, find the one that sounds like your shop, then confirm it with your processor.

SAQ type	Who it fits
SAQ A	All card handling outsourced; e-commerce or mail/phone orders
SAQ A-EP	E-commerce where your site touches the payment page
SAQ B	Imprint machine or standalone dial-out terminal
SAQ B-IP	Standalone terminal connected by internet (IP)
SAQ C	A POS application connected to the internet
SAQ C-VT	A virtual terminal — you key cards into a web page
SAQ P2PE	A listed point-to-point-encryption terminal
SAQ D	The catch-all — or if you store card data

The shortest in-person questionnaire is **SAQ P2PE**, used with a listed point-to-point-encryption terminal that scrambles the card data the instant it's read. SAQ D is the longest, and you only land there if you store card data or don't fit the simpler buckets — a good reason not to store card numbers.

★ Not sure which is yours?

This is exactly the kind of thing I'm happy to sort out with you at your counter. We'll look at how you take cards, figure out the likely SAQ, and then confirm it with your processor together. Call or text (330) 200-8042.

How your POS system does most of the work

This is the most reassuring page in the guide, so read it twice.

When you take cards through Square, Clover, Toast, or Shopify using THEIR own listed card readers and terminals, the card number is encrypted right at the reader and never sits in plain form on your equipment. That design is what keeps your questionnaire short — a big chunk of the security burden lives with the provider, not with you.

That's often why a shop using one of these systems with a listed reader lands on a short SAQ (frequently SAQ A for online, or SAQ P2PE with a listed encrypting terminal in person). Your provider publishes guidance on which SAQ its setup supports — ask them for it by name.

The catch is 'their own listed hardware.' Plug in some random off-brand reader, or key card numbers into a spreadsheet, and you can quietly push yourself onto a longer, harder questionnaire. Stay inside your provider's blessed setup and it stays simple.

✓ Use the listed reader, keep it simple

The single easiest way to keep this painless is to use the card reader your provider sells and lists. It isn't about brand loyalty — it's that the listed gear is what the short questionnaires are written for.

The part that's genuinely on you

Your POS handles the card data, but a few habits are yours to keep. These are the questions you'll actually be answering.

Strong, unique passwords

Your POS login and your bank login should each have a long, unique password you don't reuse anywhere else. A password manager makes this easy, and it's the single biggest thing most small shops can tighten up.

Turn on multi-factor authentication

Multi-factor authentication (MFA) means a second step — a code on your phone — on top of your password. Turn it on for your POS account and your bank. It's the lock that stops a stolen password cold.

Never store full card numbers yourself

Don't write card numbers on a notepad, type them into a spreadsheet, or keep them in email or texts. If you need a card on file for a repeat customer, let your POS store it as a secure token (our deposits-and-cards-on-file guide explains how). The card number should live in the system, never in your own files.

! The one that gets good people in trouble

Storing full card numbers yourself — even with good intentions, even just 'for regulars' — is the fastest way onto the longest questionnaire and the biggest risk if your records are ever lost or stolen. Let the system hold the cards. You hold the trust.

The PCI fee — and the penalty for skipping it

Two fees show up around this topic. Knowing both is why it's worth doing your questionnaire on time.

Many processors charge a **PCI fee** — a recurring charge, often monthly or yearly, tied to compliance. Whether you see one, and how much, depends entirely on your processor and plan, so check your statement. The flat-rate systems often fold this in or don't list it separately; a bank or reseller deal is more likely to bill it on its own line.

There's also a **PCI non-compliance fee** — a penalty some processors add when you haven't completed your questionnaire. It's usually larger than the compliance fee itself, which is exactly the point: they want you to do the paperwork. Our reading-your-statement guide helps you spot both of these on a real bill.

✓ Do the form, dodge the penalty

If you're paying a non-compliance fee, finishing your questionnaire usually makes it stop. It's one of the few bits of paperwork that pays for itself. Check your statement to see which fee you're being charged.

Keeping the setup around your register secure

A short questionnaire still assumes the basics are in place. Most of them are things you'd want anyway.

Keep the Wi-Fi your register uses on a private network with a strong password — not the same open network you hand out to customers. Change any default passwords on your router and devices. Keep your POS app and your devices updated so security fixes actually reach you.

If you offer guest Wi-Fi, keep it separate from the network your payment devices use. Our register-network guide walks through setting this up in plain terms — a guest network for customers, a private one for the equipment that touches money.

! Customer Wi-Fi and your register don't mix

Running your card terminal on the same open Wi-Fi you give customers is a needless risk. Keep the gear that handles payments on its own private network. It's a small change that closes a real door.

Two kinds of small business, two setups

Which questionnaire fits you depends on how and where you take cards — so a tidy storefront and a market vendor can land on different (but both short) forms.

If you sell from a fixed counter or shop

You ring people up at a counter with a listed terminal or stand from your POS provider. The card is read and encrypted right at the reader, which is what keeps your questionnaire short.

- Use the listed terminal or stand your provider sells — that's what the short SAQs are written for.
- A listed encrypting terminal often points you at the short SAQ P2PE; confirm with your processor.
- Keep the register on a private network, not the guest Wi-Fi (see our register-network guide).
- Strong unique password plus MFA on the POS account.

If you sell on the go — markets, trucks, house calls

You take cards on a phone or pocket reader at markets, trucks, or house calls. The reader still encrypts the card; your phone is just the screen, which keeps your part small.

- Use your provider's own listed reader (Square Reader, Shopify Tap and Chip, Clover Go) — not an off-brand one.
- If you take orders online or by phone too, that part may fall under SAQ A; ask your processor.
- Never jot a card number on paper at the table — let the reader or an emailed invoice do it.
- Lock your phone, keep the POS app updated, and turn on MFA.

★ Mixed setup? That's common

Lots of owners sell at a counter AND work the weekend market. That can mean more than one way of taking cards, which is worth confirming with your processor. Tell me how you sell and I'll help you sort it out. Call (330) 200-8042.

Filling in the questionnaire, step by step

When your processor sends the yearly questionnaire, here's the calm way through it.

- **Confirm your SAQ type first.** Ask your processor which SAQ your setup uses before you answer anything — it decides which questions you even see.
- **Read each question literally.** They're mostly yes/no. If you don't understand one, that's a question for your processor, not a guess.
- **Answer honestly.** A wrong 'yes' helps no one — the point is to find and fix gaps, not to perform.
- **Fix anything that's a 'no'** before you sign — turn on MFA, change a default password, move the register off guest Wi-Fi.
- **Sign and submit through your processor's portal,** and keep a copy with your business papers.
- **Do the scan if you're told to.** Some setups need a quarterly network scan from an approved vendor; your processor arranges it.

✓ Block out an hour, not an afternoon

For a typical small shop on a short SAQ, this is an hour's job once a year, not a project. Pour a coffee, close the questions one at a time, and you're done.

When you might actually want a professional

I said most small shops can do this themselves, and they can. Here's when it's fair to bring in paid help.

If you store card numbers in your own systems, run your own custom website that handles payments directly, take a very large volume, or have had a security incident, you may be on SAQ D or facing a formal assessment. That's when a Qualified Security Assessor or a security pro earns their fee.

Most of the shops I help aren't in that camp — they use a mainstream POS with a listed reader and land on a short SAQ. If you're not sure which camp you're in, that itself is the question to put to your processor: 'Which SAQ does my account use?'

★ I'll help you tell which camp you're in

You shouldn't pay a specialist for a job you don't need, and you shouldn't go it alone on a job that needs one. I'll sit with you, look at how you take cards, and help you see which it is — plainly and with no upsell. Call (330) 200-8042.

The rule that changes everything: storing card data

Everything in this guide gets harder the moment you store full card numbers. So the simplest advice is: don't.

If a full card number ever lands in your own files — a spreadsheet, a notepad, a saved email, a photo of a card — you've taken on the job of guarding it, and you've likely moved onto SAQ D, the longest questionnaire. You've also made yourself the target if those records are ever stolen.

The fix is to let your POS store cards as secure tokens instead. A token is a stand-in code that lets you charge a repeat customer without you ever holding the real number. Our deposits-and-cards-on-file guide shows how to set that up properly, so a regular's card is on file without a single digit living in your own files.

! A photo of a card is stored card data

This trips up good people: snapping a picture of a customer's card, or keeping the number in a text, counts as storing card data. Delete those, and use your POS's card-on-file feature instead. Your questionnaire — and your customers — will thank you.

Staying compliant all year, not just at form time

The questionnaire is once a year, but the habits are every day. Keep these and next year's form fills itself in.

- Keep MFA on and passwords unique — don't quietly turn them off for convenience.
- Keep your POS app and devices updated as prompts arrive.
- Never start storing card numbers 'just this once' — use card-on-file tokens instead.
- Keep the register on its private network, guests on the guest network.
- Retire old devices properly — sign out and wipe them before they leave the shop.
- Keep this year's signed SAQ with your business papers so next year is a quick update.

✓ Good habits make the form boring

The owners who dread the questionnaire are usually the ones who let the basics slide all year. Keep the small habits and the yearly form becomes a five-minute 'yes, still doing all that.'

Questions to ask your processor

You don't need to be an expert — you need to ask the right few questions. Here they are.

Q: Which SAQ type does my account use?

This is the first and most important question. The answer decides which questions you'll actually fill in. Ask them to name it (SAQ A, P2PE, and so on) in writing.

Q: Do I need a network scan, and who runs it?

Some setups need a quarterly scan from an approved vendor. Ask whether yours does and whether the processor arranges it for you.

Q: Is my card reader a listed, encrypting device?

Using your provider's listed reader is what keeps your questionnaire short. Confirm the exact reader you have qualifies.

Q: Am I being charged a PCI fee or a non-compliance fee?

Ask which one appears on your statement. If it's a non-compliance fee, finishing your questionnaire usually stops it.

✓ Get the SAQ name in writing

A friendly 'oh, you're fine' over the phone isn't the same as being told your SAQ type in writing. Ask for the specific name so you fill in the right form and have a record of it.

Common mistakes people make

A few avoidable slip-ups cause most of the trouble here. Now you'll spot them coming.

- **Ignoring the yearly email** and quietly racking up a non-compliance fee month after month.
- **Storing card numbers** in a spreadsheet, notepad, or photo instead of using card-on-file tokens.
- **Using an off-brand reader** that pushes them off the short questionnaire onto a longer one.
- **Running the register on open guest Wi-Fi** instead of a private network.
- **Guessing at answers** instead of asking the processor which SAQ applies and what a question means.
- **Paying a consultant** for a short SAQ a small shop could complete itself in an hour.

! The costliest mistake

The one that actually hurts is storing card data you didn't need to. It lengthens your questionnaire AND makes you the target in a breach. If you take one thing from this guide: let the system hold the cards, never your own files.

Why this is worth ten minutes of your attention

It's easy to treat the questionnaire as a nuisance. Here's the honest case for caring a little.

The card number you take from a customer is a piece of their trust. The whole standard exists so that trust doesn't leak. Doing your part — a short form, strong passwords, MFA, no stored card numbers — is how you keep faith with the people who shop with you.

And there's a plainer reason: skipping it can cost you a penalty fee every month, and a real security slip could cost you far more than that. Ten minutes of good habits is cheap insurance against an expensive bad day.

★ Small shops can absolutely do this

I've helped plenty of owners who were sure they'd need to hire someone, and nearly all of them were done in an afternoon with the basics squared away. You've got this — and if you'd like a hand the first time, that's what I'm here for. Call (330) 200-8042.

Where to confirm the current rules

Versions and details change, so here's where the real answers live — not a forum or a sales pitch.

The **PCI Security Standards Council** publishes the standard and every SAQ form on its official site. It's the source of truth for which version is current and what each questionnaire asks. As of late 2026 the version is v4.0.1 — but always confirm you're on the current one.

For the form that applies to YOUR business, though, your **processor** is the one to ask — Square, Clover, Toast, Shopify, or your bank each publishes guidance for its own setup and tells you which SAQ it supports. Between the Council for the standard and your processor for your specifics, you've got everything you need.

✓ Two trustworthy sources, no noise

Stick to the PCI Security Standards Council for the standard and your own processor for your setup. Those two will steer you right. Skip the scary blog posts trying to sell you a service you may not need.

Turning it into a simple yearly routine

The owners who never stress about this have turned it into a habit. Here's a routine you can copy.

Pick a month — say, the one your processor usually emails you — and treat it as your card-security month. Set a reminder. When the questionnaire arrives, you confirm your SAQ type, run through the questions, fix any 'no', sign, and file a copy. Done for a year.

While you're at it, do a quick once-over: are passwords still unique, is MFA still on, is the POS app updated, are you still not storing card numbers? Five minutes of housekeeping keeps next year's form easy and keeps your shop genuinely safer, not just on paper.

✓ File it with your tax papers

Keep your signed questionnaire with your yearly business paperwork — the same drawer as your tax documents. Then it's right where you'll look for it and easy to reference the following year.

Setting honest expectations

Let's be clear about what doing your questionnaire does and doesn't promise, so you feel settled about it.

Completing your SAQ confirms you're following the standard and keeps you in good standing with your processor. It's the right thing to do and it meaningfully lowers your risk. What it can't do is promise that nothing will ever go wrong — no checklist can. It makes a bad day far less likely and far less severe.

Expect the process to feel unfamiliar the first time and routine every time after. Expect to lean on your processor for the specifics, because that's what they're there for. And expect that keeping good daily habits matters more than the form itself.

✓ Progress, not perfection

You don't have to be a security expert. You have to take cards through a trustworthy system, keep a few good habits, and answer honestly once a year. That's a bar a careful small-business owner clears easily.

Common Questions

The questions I hear most from owners facing their first card-security questionnaire, answered plainly.

Q: Do I really have to do this if I'm tiny?

Yes — the questionnaire is based on how you take cards, not how big you are. The good news is that the smallest, simplest setups get the shortest forms. Confirm your SAQ type with your processor.

Q: Do I need to hire a consultant?

Usually no. A typical small shop on a mainstream POS with a listed reader lands on a short SAQ it can complete itself. Paid help makes sense mainly if you store card data or face a formal assessment.

Q: Does using Square, Clover, Toast, or Shopify mean I'm compliant?

It does most of the heavy lifting, but not all of it. You still keep your account secure — strong unique passwords, MFA, no stored card numbers — and you still complete your yearly questionnaire.

Q: What's the current version I should mention?

As of late 2026 it's PCI DSS v4.0.1, with its future-dated requirements in effect since March 31, 2025. Always confirm the current version on the PCI Security Standards Council site or with your processor.

★ Still feels like a lot?

It's a favorite thing of mine to help with, because I get to turn something scary-sounding into a short, doable task at your own counter. Call or text me at (330) 200-8042 and we'll knock out your questionnaire together.

You don't have to figure this out alone

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

I hope this guide made the card-security questionnaire 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 feel you have to memorize a thing.

When you'd rather have a hand, that's exactly what I do. I come to your shop or your kitchen table, 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 don't sell payment processing and I earn no commission from any company — so the advice you get is just honest advice. For the tax and legal fine points, I'll point you to your accountant or attorney.

★ 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

Which Questionnaire Fits How You Take Cards

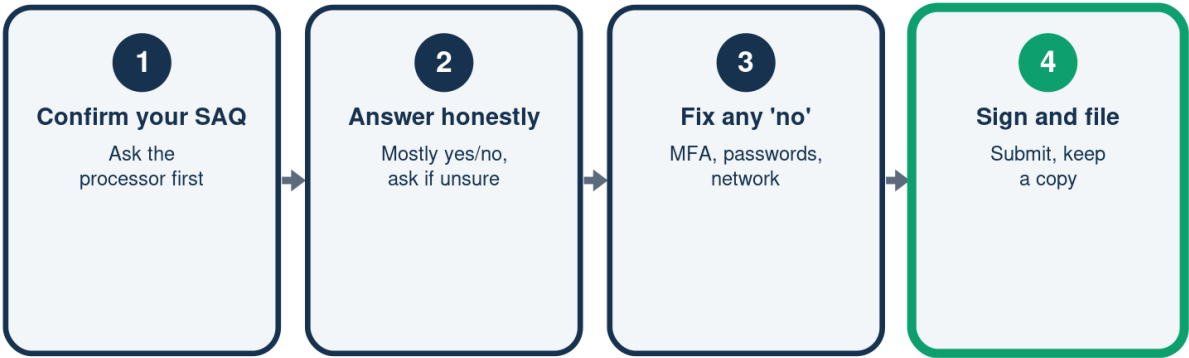
Your SAQ follows your setup, not your size

	How you take cards	Likely short SAQ
Listed encrypting terminal	In person	SAQ P2PE
All handling outsourced	Online / MOTO	SAQ A
Standalone IP terminal	Dial or internet	SAQ B-IP / B
You store card data	Avoid this	SAQ D (longest)

Confirm your exact SAQ type with your processor before you file.

Doing Your Questionnaire in Four Steps

The calm once-a-year routine



For a short SAQ this is about an hour, once a year.

What the System Handles vs. What's on You

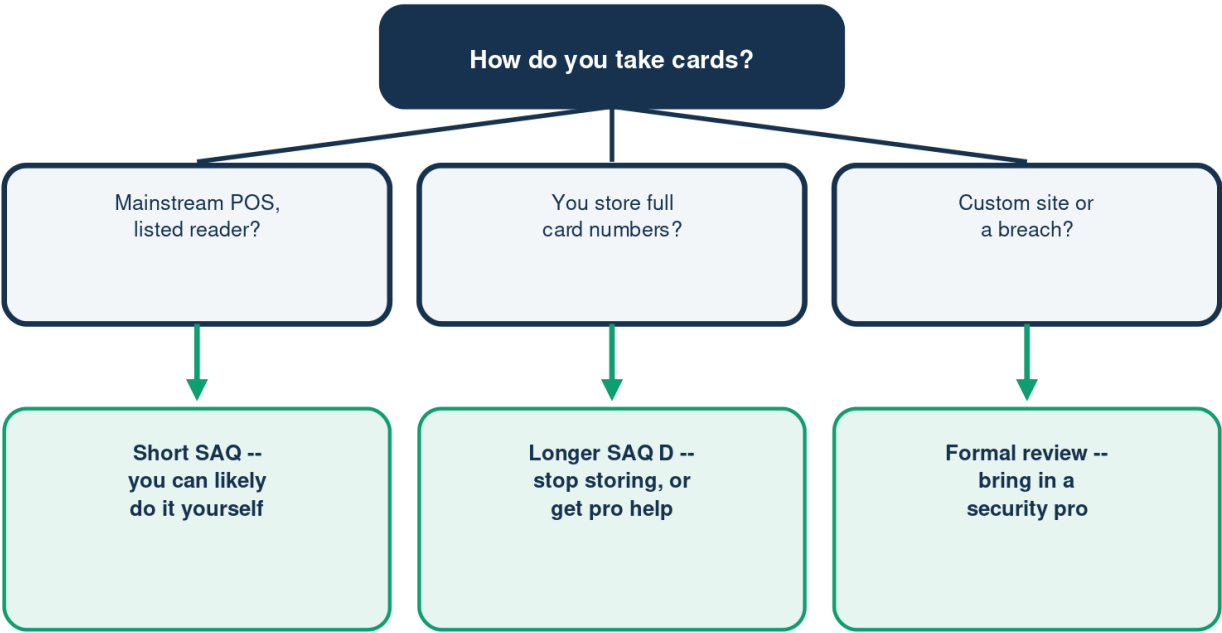
The less card data you touch, the shorter your form

	Your POS provider	You
Encrypt the card	Yes	--
Strong unique passwords	--	Yes
Turn on MFA	--	Yes
Never store card numbers	Helps via tokens	Your habit

Use the listed reader and let the system hold the cards.

Do You Need to Pay for Help?

Most small shops don't -- here's how to tell



Version and rules change -- confirm current with your processor.

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