



An Extended Guide · No. 2073

Ohio's Data Protection "Safe Harbor": How a Written Program Protects You

The legal reward Ohio offers
for taking security seriously

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. Ohio law adds one more reason to do those basics on paper: a written security program can become a legal shield if you are ever sued over a breach.

The reward Ohio offers for doing security right

Ohio has a law that most small-business owners have never heard of, and it works in your favor. If you put a real, written security program in place, the state gives you a legal defense you can raise if someone sues you after a data breach. It is called a safe harbor, and this guide explains it in plain English.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. For 30-plus years I've helped folks and small businesses get comfortable with their technology. I'm a tech helper, not a lawyer — so think of this as me explaining the idea at your kitchen table, then pointing you to the right professional to make it official.

The short version: this is a carrot, not a stick. There's no penalty for skipping it. But the same written plan that earns you this legal protection is the plan that actually keeps you safer day to day — so you win either way. That's rare in the world of rules.

★ I can help you build the program, not just talk about it

The legal wording is for a lawyer, but the hands-on part — turning on the safeguards, writing down what you do, keeping proof — is exactly my job. I can get the practical side in place so your attorney has something real to work with. Call or text me at (330) 200-8042.

The whole guide, on one page

If you remember only these things, you'll understand what Ohio's safe harbor is and why it's worth your while.

- ❑ Ohio's Data Protection Act (in **ORC chapter 1354**) offers a legal **safe harbor** to businesses that keep a written security program.
- ❑ It's an **affirmative defense** — something you can raise in a lawsuit — not immunity and not a government certificate.
- ❑ It's **voluntary**. There's no fine for not having one; it's a reward for doing the work.
- ❑ To qualify, you create, maintain, and follow a **written** program with administrative, technical, and physical safeguards.
- ❑ That program must **reasonably conform to a recognized framework** (like NIST, CIS, or ISO) and scale to your size and your data.
- ❑ The exact legal scope is a lawyer's call — confirm whether and how you qualify with an **Ohio attorney**.

✓ The plan does double duty

Everything the safe harbor asks for is good security anyway. Even if you're never sued, you end up with a tested, written plan that protects your business. Our 'One-Page Security Plan' guide is a friendly place to start.

What the Data Protection Act actually gives you

Let's start with what Ohio put on the table, in everyday terms.

Ohio passed the Data Protection Act — it began as Senate Bill 220 and took effect back in November 2018. It lives in the Ohio Revised Code at chapter 1354, with the core requirements in section 1354.02. You don't need to read the statute; you just need the idea behind it.

The idea is this: if your business keeps a genuine written cybersecurity program, and someone later sues you in Ohio claiming your weak security caused a breach, you can raise that program as a **defense**. You're telling the court, in effect, 'I did take reasonable, recognized steps — here's the written proof.'

It's the state's way of rewarding businesses that invest in security ahead of time instead of waiting for disaster. The law doesn't demand perfection; it rewards a reasonable, documented effort.

! 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.

An affirmative defense — not a force field

The single most important thing to understand is exactly what kind of protection this is, so you don't over- or under-rely on it.

An **affirmative defense** is a legal argument you can raise if you're sued. It doesn't stop a lawsuit from being filed, and it doesn't promise you'll win automatically. It gives your attorney a strong, Ohio-recognized position to stand on: that you had a reasonable written security program in place.

So think of it as armor you put on before a fight might happen — not a wall that keeps the fight from ever starting. If no one ever sues you, you never need to use it. But the day you might need it, you'll be very glad it's there and in writing.

! It protects against certain Ohio tort claims — not everything

The safe harbor is aimed at tort claims brought under Ohio law that allege your failure to use reasonable security caused a breach. It is not a shield against every possible legal or regulatory problem, and other rules can still apply. Whether it covers your specific situation is a legal question — that's a conversation for an Ohio attorney.

Three things the safe harbor is NOT

Clearing up the common misunderstandings saves you from false comfort — and from skipping it for the wrong reason.

It is not immunity

It doesn't make you untouchable. It gives you a defense to raise, and that defense still has to be argued. It also doesn't cover breaches caused by things outside the law's reach.

It is not a government certification

No state office inspects your business and hands you a certificate. You build and keep the program yourself (with help from folks like your lawyer and me). The proof that it exists is your own documentation.

It is not required

It's completely voluntary. Ohio won't fine you for skipping it. That's why I call it a carrot: you do the work because it protects your business two ways — better security now, and a legal defense later.

✓ Voluntary doesn't mean optional-in-spirit

Because there's no penalty, it's easy to put off forever. Treat it like testing your backups: nobody makes you, but the people who do it sleep better. Our backup fire-drill guide makes that same case.

What a qualifying program has to cover

At its heart, the program has to protect your information across three kinds of safeguards. Here's what each means in plain terms.

Safeguard	In plain English
Administrative	Your rules and habits — who can see what, training, and your plan for when something goes wrong.
Technical	The computer settings — MFA, encryption, antivirus, updates, access controls on accounts and devices.
Physical	The real-world locks — who can get to the computers, the server, paper files, and backup drives.

A real program touches all three. Most owners already do pieces of each — a lock on the office door, a password on the laptop, a rule about who opens the mail. The program just gathers those into one written, deliberate whole and fills the gaps.

★ **We'll cover all three, not just the computer part**

People forget the physical and the human sides. In one visit I can walk your space, check the technical settings, and help you write down the everyday rules — so all three safeguards are real, not just the flashy one. Call (330) 200-8042.

The recognized frameworks you can build on

You don't invent your own standard. Your program has to reasonably conform to one of the recognized frameworks the law points to.

A framework is just a published, respected checklist of security practices. Ohio's law names several so you can pick the one that fits. You don't have to memorize them — your attorney and I can help you choose. Here are the main families it recognizes:

- **NIST** — the NIST Cybersecurity Framework (CSF), plus NIST SP 800-171 and 800-53. Plain-language, small-business-friendly versions exist.
- **CIS Critical Security Controls** — a practical, prioritized list that's popular with smaller shops.
- **ISO 27000 series** — the international information-security standard, common with larger or global businesses.
- **FedRAMP** — for those working with federal cloud requirements.
- If you're already regulated: compliance with the **HIPAA Security Rule**, **GLBA / FTC Safeguards**, or **PCI-DSS** can serve as the basis instead.

✓ Already follow one of these? You may be most of the way there

If you're a tax preparer under FTC Safeguards, a clinic under HIPAA, or a card-taking shop under PCI-DSS, your existing written plan may double as your safe-harbor basis. Our FTC Safeguards and PCI guides explain those.

It scales to your business — on purpose

Here's the part that makes this reachable for a two-person shop: the law expects your program to fit your size.

The program is meant to match the size and complexity of your business and the sensitivity of the data you hold. A solo bookkeeper handling Social Security numbers isn't expected to have the same setup as a hospital. The standard is **reasonable for you**, not enterprise-grade for everyone.

That's genuinely good news. It means a small business can build a real, qualifying program without a giant budget or a full-time IT department. The point is a thoughtful, honest, written effort that's right-sized — not a pile of expensive tools you'll never use.

! Right-sized still has to be real

Scaling down doesn't mean skipping the essentials. MFA everywhere, tested backups, current updates, and basic access control are the baseline at any size — those are the controls that actually stop breaches, and a program without them isn't reasonable no matter how small you are.

What a right-sized program looks like for you

The three safeguards apply to everyone, but what counts as reasonable looks very different for a one-person shop than for a team that holds piles of customer records.

If you're a solo operator or tiny shop

Your program can be short and plain. The goal is to show you made a deliberate, written, reasonable effort that follows a recognized framework scaled to one or two people.

- Pick a small-business-friendly framework like the CIS Controls or the NIST CSF Quick-Start and follow it at your scale.
- Write a few pages: what data you hold, your safeguards, and what you'd do in an incident.
- Turn on MFA, encrypt your laptop, keep a tested backup — then write down that you did.
- Review and date it once a year so it stays current.

If you have staff and handle sensitive data

More people and more data mean a fuller program: training records, access lists, and a real incident-response plan. The framework you pick should reflect the kind of data you hold.

- Document who can access what, and cut access the day someone leaves (see our offboarding guide).
- Keep training records — showing staff were taught to spot scam emails is part of the administrative safeguards.
- Separate administrator accounts from everyday ones, and log that choice in your program.
- Match your framework to your data: HIPAA for health info, FTC Safeguards for financial, and so on.

★ Not sure what 'reasonable' means for your size?

Tell me how your business runs and what data you keep, and I'll help you figure out a right-sized program — real enough to qualify, light enough to actually maintain. Call (330) 200-8042.

How you qualify, step by step

There's no form to file. You qualify by actually doing — and documenting — these things.

- ❑ **Pick a recognized framework** that fits your size and the data you hold.
- ❑ **Build the three safeguards** — administrative, technical, and physical — to reasonably conform to that framework.
- ❑ **Write it down** in a real document: what you protect, how, and who's responsible.
- ❑ **Follow it** — a plan you don't actually comply with won't help you.
- ❑ **Maintain it** — review and update it as your business and the threats change.
- ❑ **Keep proof** — dated records that show the program existed and was being followed.

Notice there's no government step in that list. You're not applying for anything. You're building something real and keeping the receipts, so that if the day ever comes, your attorney can show the court you were serious.

What 'reasonably conforms' really means

That phrase does a lot of work in the law, so it's worth understanding what it asks — and what it doesn't.

To conform reasonably to a framework, your program should genuinely follow its practices in a way that makes sense for your business. It does **not** mean you must check every single box a framework lists, especially the ones built for giant organizations. It means a fair, honest fit.

This is where a professional earns their keep. A lawyer who knows Ohio law, sometimes with a security advisor, can help you judge whether your program reasonably conforms — because that judgment is exactly what a court would weigh. It's not something to guess at alone.

! A binder you ignore does not 'conform'

The deadliest version of this is a nice-looking document that describes controls you never actually turned on. 'Reasonably conforms' means you both wrote it **and** live by it. A plan on the shelf that doesn't match reality can hurt more than help.

Putting the program on paper

The word 'written' is in the law for a reason. Here's how to make the document useful instead of a chore.

Your program should be a real document you can hand to someone. It doesn't need legal language or a hundred pages. A clear, dated plan that a new employee could read and understand is worth more than a thick binder of jargon nobody opens.

- Name the data you hold and where it lives.
- Name the framework you're following.
- List your safeguards under the three headings — administrative, technical, physical.
- Say who's responsible for security and what happens in an incident.
- Date it, and note when you'll review it next.

✓ Start small and grow it

A short honest plan you keep current beats a perfect one you never finish. Our 'One-Page Security Plan' guide gives you a friendly skeleton you can expand into a full program over time.

Maintaining and complying — the quiet half

Writing the program is the start. The law also asks that you maintain it and comply with it, and that's where most of the real value is.

Maintaining means keeping it current: when you add a service, hire someone, or change how you work, the program should keep up. A quick yearly review — re-read it, fix what's stale, re-date it — is usually enough for a small business.

Complying means you actually do what it says. If your plan promises MFA everywhere and tested backups, those have to be true in real life. The gap between a plan and reality is exactly what a defense attorney doesn't want to explain to a court.

★ Put me on your yearly calendar

A lot of owners ask me to swing by once a year to re-check the settings, confirm the plan still matches reality, and help re-date it. It's a short visit that keeps your program honest and current. Call (330) 200-8042.

The technical safeguards that carry the most weight

No matter which framework you pick, a handful of technical controls show up on every list — and they're the ones that actually stop breaches.

- **MFA everywhere** — a second sign-in step on email, cloud, remote access, and admin accounts. The single biggest win.
- **Tested backups** — kept offline or isolated, and actually restored at least once so you know they work.
- **Current updates** — security patches installed, and end-of-support software replaced.
- **Disk encryption** — BitLocker on Windows, FileVault on Mac, so a lost laptop isn't a breach.
- **Least privilege** — everyday accounts separate from administrator accounts, access only where needed.

Do these and document them, and you've covered the heart of the technical safeguards for a small business. Our Microsoft 365 and Google Workspace guides walk through turning on MFA; the backup fire-drill guide covers testing a restore.

Where a lawyer comes in — and where I do

This is a legal protection, so let's be clear about who does what, so you line up the right help.

An **Ohio attorney** is the right person to confirm whether the safe harbor applies to your business, whether your program reasonably conforms, and how to position it if you're ever sued. The whole value of this is legal, so the legal judgment belongs with a lawyer. This guide is general information, not legal advice.

My job is the hands-on side: turning on the safeguards, helping you write down what you actually do, keeping dated proof, and testing that the controls work. I give your lawyer something real to point to. We make a good team — you shouldn't have to pay lawyer rates for someone to flip on MFA.

✓ Ask your attorney these questions

Does the safe harbor apply to my business? Which framework fits my size and data?
Does my written program reasonably conform? Bring your dated plan to that meeting and the conversation goes faster.

The pitfalls that undo a program

A program only protects you if it's real and current. These are the slips I see most often.

- **Writing a plan you don't follow** — the single biggest mistake. The document must match reality.
- **Letting it go stale** — an undated plan from years ago that no longer describes your business.
- **Picking a framework and ignoring it** — naming NIST but not actually doing its practices.
- **Skipping the physical and human safeguards** — all computer settings, no locks or training.
- **No proof** — no dated records that the program existed and was being followed.

! The wrong time to discover a gap is in a lawsuit

If a breach leads to a claim, your program gets examined closely. A plan that promised controls you never turned on can leave you worse off than no plan at all. Keep it honest, keep it current, keep the proof.

The benefits even if you're never sued

Here's why I tell every owner this is worth doing regardless of the legal angle.

The honest truth is most small businesses will never use the safe harbor in court. But building the program still pays off every single day. You end up knowing exactly what data you hold, where it lives, and how it's protected — which means fewer surprises and faster recovery if something goes wrong.

It also makes other things easier. A written program is most of what a cyber-insurance application asks for, and it overlaps heavily with the rules tax preparers, clinics, and card-takers already face. Do it once and you've covered several bases at once. Our cyber-insurance application guide shows that overlap.

✓ One plan, many payoffs

Legal defense, easier insurance, faster recovery, calmer staff. The safe-harbor program is one of the few security chores that quietly helps in half a dozen directions at once.

How to get started this month

You don't have to do it all at once. Here's a calm order that gets you to a real program without overwhelm.

- ❑ **Week one:** write down the data you hold and where it lives. You can't protect what you haven't listed.
- ❑ **Week two:** turn on the technical baseline — MFA, encryption, updates, a tested backup.
- ❑ **Week three:** pick a right-sized framework and sketch your program under the three safeguards.
- ❑ **Week four:** write the short incident plan and the yearly-review note, then date it.
- ❑ **Then:** take the dated program to an Ohio attorney to confirm it reasonably conforms for your business.

Four short steps and you have something real. It won't be perfect, and that's fine — a reasonable, honest, written effort is exactly what the law asks for, and you can keep improving it each year.

Keeping the proof that the program is real

Because there's no certificate, your own records are the evidence. A little filing habit now is what makes the defense usable later.

For each safeguard in your program, keep a simple dated record that shows it's true: a screenshot of MFA enforced, the date you tested a restore, your training sign-in sheet, your access list. These aren't busywork — they're the receipts that turn 'we had a program' into 'here's the proof.'

Store them where you can find them and where a crisis can't erase them — a labeled folder on a backed-up drive, plus a printed copy with your business papers. Keep the old dated versions when you update, so you can show the program existed over time.

★ I'll set up the evidence folder with you

The proof is easy to gather while we're already turning things on — a screenshot here, a dated note there. In one visit we can build the folder so your lawyer has everything in one place. Call (330) 200-8042.

Why the written program is worth the afternoon

Set the two paths side by side and the choice gets simple.

Without a written program, if you're ever sued over a breach, you're arguing from scratch — hoping to convince a court your security was reasonable, with no framework and no dated proof to point to. With one, your attorney has a recognized, Ohio-specific defense ready to raise, backed by documents you prepared calmly, long before any trouble.

And remember the day-to-day payoff doesn't depend on a lawsuit at all. The same program that would defend you is the program that keeps the breach from happening in the first place, speeds your recovery if it does, and smooths your insurance and compliance paperwork along the way.

✓ The best time to build it is before you need it

You can't create a safe-harbor program after a breach to cover a breach that already happened. Like a backup or a smoke detector, it only helps if it's already in place. An afternoon now buys real peace of mind.

Common Questions

The questions owners ask me most about Ohio's safe harbor, answered plainly. Remember: general information, not legal advice.

Q: Do I have to register with the state to get the safe harbor?

No. There's no filing and no certificate. You qualify by building, following, and documenting a real written program that reasonably conforms to a recognized framework. Your own dated records are the proof.

Q: Is my little one-person business too small for this?

Not at all — the law expects the program to scale to your size. A solo shop can have a short, plain program that still qualifies, as long as it's real and follows a right-sized framework.

Q: Does having the program mean I can't be sued?

No. It doesn't stop a lawsuit from being filed. It gives your attorney a strong defense to raise if you are sued over a breach — that you had a reasonable written program. That's why it's called a safe harbor, not immunity.

Q: Which framework should a small business pick?

Many small shops do well with the CIS Controls or a NIST CSF Quick-Start because they're practical and plainly written. If you're already under HIPAA, FTC Safeguards, or PCI-DSS, that can serve as your basis. Confirm the fit with your attorney.

Q: How often do I have to update it?

The law asks you to maintain it; for most small businesses a yearly review — plus updates whenever something big changes — keeps it current. Re-date it each time so you can show it stayed alive.

★ Want a hand turning this into a real program?

I'll help you build and document the hands-on side so your attorney can confirm the legal side. Plain English, no jargon, nothing to sell you. 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 Ohio's data-protection safe harbor 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

What the Safe Harbor Is

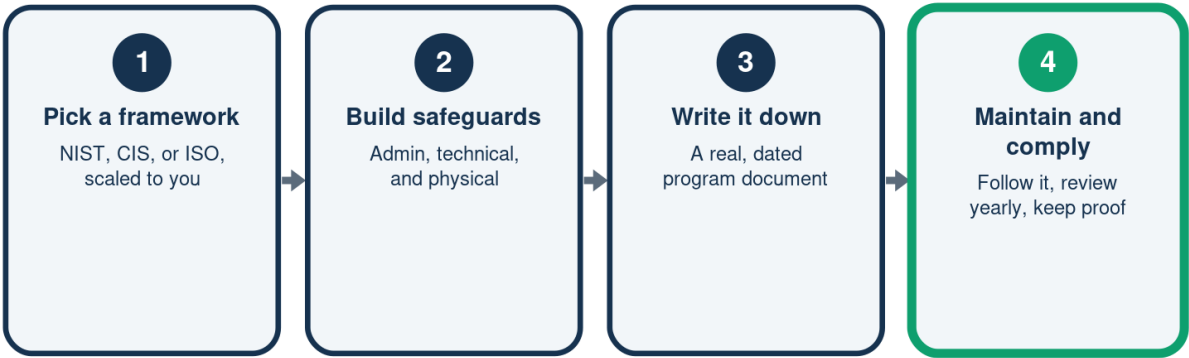
Clearing up the biggest misunderstanding

	People think	It actually is
The protection	A force field	A legal defense
Who grants it	The state	You, by doing it
Is it required	Mandatory	Voluntary reward
Proof it exists	A certificate	Your dated records

An affirmative defense you can raise if sued -- not immunity.

How You Qualify

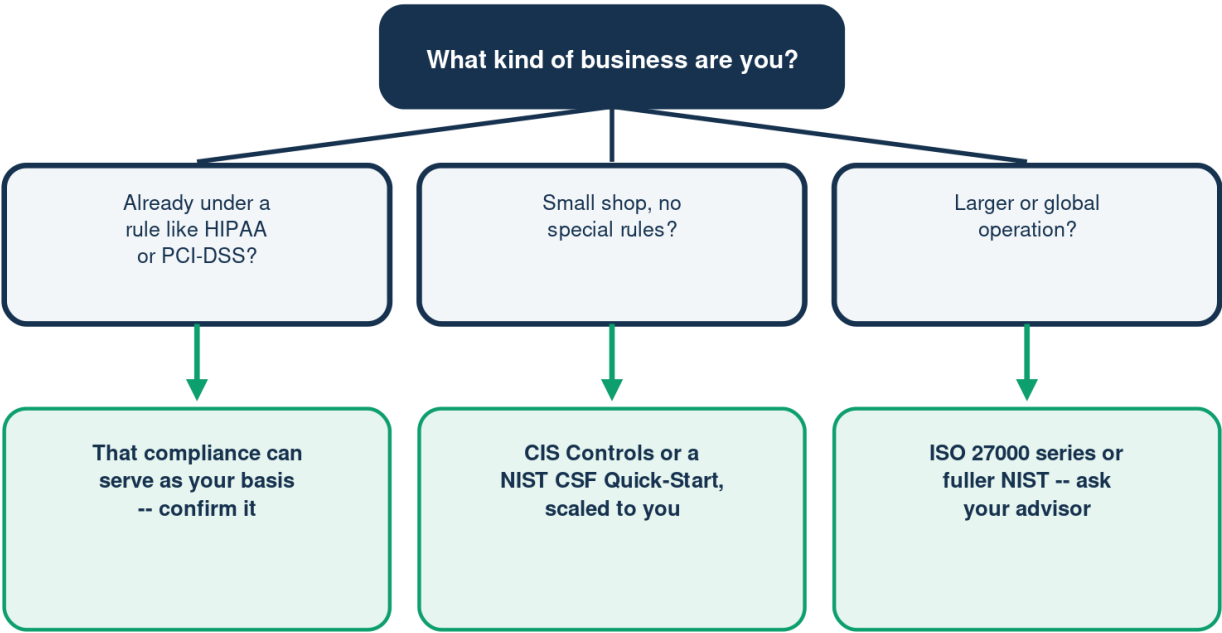
No form to file -- you qualify by doing



A reasonable, documented effort -- confirm the fit with an Ohio attorney.

Which Framework Fits You?

Start from what you already do



Naming a framework is not enough -- you must actually follow it.

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

The Three Safeguards

A real program touches all three

Safeguard		Example
Administrative	Rules and training	Who sees what
Technical	MFA, encryption	Updates, backups
Physical	Locks and access	Where devices live

All computer settings and no locks or training is not a full program.



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