



An Extended Guide · No. 2075

Townships, Villages & Schools: Ohio's Cybersecurity Program Requirement

What local public bodies must adopt,
report, and decide — in plain English

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. For a township, village, or school office, that groundwork is now also the law: Ohio requires public bodies to adopt a cybersecurity program and to report incidents on a tight clock.

New rules for townships, villages, and local offices

If you serve a township, a village, a county office, or a school, Ohio now has cybersecurity rules written specifically for public bodies. There's a program your board needs to adopt, tight deadlines for reporting an incident, and a special rule about ransom payments. This guide explains it all in plain English.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. I've spent 30-plus years helping folks and small organizations with their technology. I'm a tech helper, not a lawyer — so I'll explain what the law asks and help with the hands-on parts, while your legal counsel and the Auditor of State's office confirm the official details.

I know small public offices are stretched thin — often one or two people wearing a dozen hats, running on a tight budget. The good news is that the core of what the law wants is the same sensible security any small operation needs, just written down and adopted on the record. We'll take it one piece at a time.

★ I help local offices, not just businesses

Townships and village offices call me for exactly this kind of thing — turning on the protections, writing down the program, and getting ready to report fast if something happens. Plain English, patient pace. Call or text me at (330) 200-8042.

The whole guide, on one page

If you remember only these things, you'll know the shape of Ohio's public-body cybersecurity rules.

- ❑ Ohio's political-subdivision cybersecurity law (**ORC 9.64**) took effect **September 30, 2025**.
- ❑ It applies to **political subdivisions** — counties, townships, and villages/municipalities. (Schools should confirm their exact status.)
- ❑ Your **legislative authority** must formally **adopt a cybersecurity program** protecting your data and systems.
- ❑ After an incident, report to **Ohio Homeland Security no later than 7 days**, and to the **Ohio Auditor of State no later than 30 days**.
- ❑ You **may not pay a ransom** unless your legislative authority formally approves it by resolution or ordinance.
- ❑ The **Auditor of State** issued guidance (Bulletin 2025-007); confirm the current specifics with their office.

✓ The two clocks are the thing to memorize

Seven days to Ohio Homeland Security, 30 days to the Auditor of State. Write those two numbers where whoever answers the phone can see them — they're the deadlines that catch offices off guard.

What Ohio now asks of public bodies

Let's start with the big picture of what changed and why.

Ohio added a section to the Revised Code — ORC 9.64 — that took effect September 30, 2025. It sets cybersecurity expectations for political subdivisions: the local governments that run our counties, townships, and villages. Local offices hold a lot of sensitive information and run services people depend on, so the state wants them prepared, not improvising.

The law has three practical parts, and we'll take each in turn: adopt a written cybersecurity program, report incidents on a set timeline, and follow a special rule before paying any ransom. None of it is exotic — it's mostly putting good practice on the record.

Where this guide names a date, a deadline, or a bulletin, treat it as a starting point and confirm the current requirement with your legal counsel and the Auditor of State's office. Rules like this get updated, and you want to be working from today's version.

! 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.

Does this apply to your office?

The law is aimed at political subdivisions. Here's how to tell whether that's you.

A political subdivision is a unit of local government — counties, townships, and villages or municipalities are the clearest examples, and the law reaches many local public bodies. If you're a township fiscal officer, a village clerk, or a county office, you should assume you're in scope and confirm the specifics with your counsel.

Schools and school districts are a common question. They should **confirm their exact status and any overlapping rules** rather than assume — education entities sometimes have their own separate requirements layered on top. When in doubt, ask your legal counsel and the Auditor of State's office which rules apply to you specifically.

✓ Not sure where you fit? Ask before you guess

The safest move for any local office is to check with your legal counsel and the Auditor of State. Two minutes of asking beats months of assuming you were exempt when you weren't.

Part one: adopt a cybersecurity program

The heart of the law is a written program your governing board formally adopts. Here's what that means in practice.

Your legislative authority — the board of trustees, village council, or county commissioners — needs to adopt a cybersecurity program that protects the **availability, confidentiality, and integrity** of your data and IT systems. In plain terms: keeping your systems running, keeping private information private, and keeping your records accurate and untampered.

'Adopt' is the operative word. This isn't just the clerk quietly turning on some settings — it's the board putting a program on the record, in the minutes, as official policy. That formal adoption is part of what the law asks for, and it's what an auditor will look for.

! A program is more than an antivirus subscription

Protecting availability, confidentiality, and integrity means real controls: MFA on logins, tested backups kept offline, current updates, access limited to who needs it, and a plan for incidents. Buying one piece of software isn't a program — the whole set, written down and adopted, is.

What a sensible program includes

You don't have to invent this from scratch. A good small-office program covers a handful of practical areas.

- **Who's responsible** — name the person or role that owns cybersecurity, even if it's shared.
- **What you protect** — a list of your systems, data, and where the sensitive records live.
- **Access control** — MFA on logins, individual accounts (no shared passwords), access only where needed.
- **Backups** — offline or isolated copies you've actually tested by restoring.
- **Updates** — security patches installed, end-of-support equipment replaced.
- **Training** — staff shown how to spot scam emails; Ohio has long tied in security-awareness training for local-government employees.
- **Incident response** — who to call and the reporting clocks, written down before you need them.

Lean on recognized frameworks (like the NIST Cybersecurity Framework or the CIS Controls) and free help from CISA and CyberOhio to shape it. Our guide on free government cybersecurity help points you to those resources, and our 'One-Page Security Plan' guide gives you a friendly starting skeleton.

Part two, first clock: 7 days to Homeland Security

If you're hit by a cybersecurity or ransomware incident, the first reporting deadline comes fast.

You must report the incident to the Executive Director of **Ohio Homeland Security** (part of the Ohio Department of Public Safety) as soon as possible, and **no later than 7 days** after you discover it. Seven days sounds like a while until you're in the middle of an incident — then it goes quickly, which is exactly why you prepare the contact information now.

'As soon as possible' carries weight alongside the 7-day cap. The state wants to know quickly so it can help and so it can watch for the same attack hitting other public bodies. Reporting promptly isn't just compliance — it's helping protect your neighbors' offices too.

! The clock starts at discovery — note the moment

The 7-day deadline runs from when you discover the incident, so the instant you realize something's wrong, write down the date and time. Keep the Homeland Security reporting contact on your emergency card so nobody loses a day hunting for it.

Part two, second clock: 30 days to the Auditor of State

There's a second report, to a second office, on a longer clock — and it's easy to overlook once the crisis cools down.

You must also report the incident to the **Ohio Auditor of State** as soon as possible, and **no later than 30 days** after discovery. The Auditor of State oversees how public money and public systems are managed, so they need to know when a subdivision has been hit.

Don't let the longer window fool you into forgetting it. Once systems are back up and the panic fades, the 30-day report is the one offices most often let slip. Put it on the calendar the day you discover the incident, right next to the 7-day one, so both get done.

✓ Two reports, two offices — track them together

The moment you discover an incident, open a simple log and write both deadlines at the top: 7 days to Ohio Homeland Security, 30 days to the Auditor of State. Check each off when it's filed, and keep proof you filed.

What this looks like for an office like yours

The law is the same, but a tiny township office and a larger county department face it with very different resources — so the practical path looks a little different for each.

If you're a tiny township or village office

With one or two staff and no IT department, keep the program lean and real. The board still has to adopt it, but it can be short, plain, and built on free frameworks and help.

- Start from a small-office framework (NIST CSF Quick-Start or the CIS Controls) scaled to a couple of people.
- Lean on free help — CISA's services and CyberOhio — so cost isn't the blocker.
- Get the board to adopt the written program on the record, in the minutes.
- Keep the two reporting deadlines and contacts taped where whoever answers the phone can see them.

If you're a larger office or district

More systems, more staff, and more sensitive records mean a fuller program and a real response plan — and schools especially should confirm which overlapping rules apply to them.

- Document your systems and data, assign a responsible person or role, and keep training records.
- Build a tested incident-response plan with named roles and the reporting clocks baked in.
- Coordinate with your IT provider on backups, MFA, and monitoring — and keep control of the master credentials.
- Schools and districts: confirm your exact status and any separate education rules with counsel and the Auditor of State.

★ Short-staffed and not sure where to start?

I work with small local offices all the time. I can help you stand up the practical program, lean on the free state and federal help, and get your reporting contacts ready — without blowing the budget. Call (330) 200-8042.

Part three: the rule before you pay any ransom

This is the piece unique to public bodies, and it's worth understanding clearly before you ever face it.

If your office is hit by ransomware, the law says a subdivision **shall not pay** or comply with a ransom demand **unless** its legislative authority formally approves the payment — by resolution or ordinance that states why paying is in the subdivision's best interest. In other words, no one person can quietly decide to pay; the board has to vote it on the record.

There's real wisdom in that. Paying a ransom is a serious decision with legal, financial, and even sanctions risk, and it never guarantees you get your data back. Forcing a public, deliberate vote slows everyone down and makes sure the decision is made with eyes open, not in a panic at 2 a.m.

! No quiet payments — the board must vote, on the record

Even under enormous pressure from attackers, a subdivision can't just pay. The legislative authority must approve it formally, in a resolution or ordinance explaining why it's in the public's best interest. Build that into your incident plan so everyone knows the rule in advance.

What to do the moment an incident hits

Preparation pays off most in the first hour. Here's the calm order for a public office, tying the deadlines together.

- ❑ **Stay calm and isolate** affected machines from the network — but don't power them off or wipe them (forensics may need them).
- ❑ **Note the date and time** you discovered it — both clocks start now.
- ❑ **Call your cyber-insurer's hotline** if you have one, and your IT help.
- ❑ **Report to Ohio Homeland Security** within 7 days.
- ❑ **Report to the Ohio Auditor of State** within 30 days.
- ❑ **Do not pay any ransom** unless and until your legislative authority formally votes to approve it.
- ❑ **Report the crime** to the FBI at ic3.gov, and use CISA's StopRansomware.gov for free help.

Our guide 'The First Hour After a Hack' walks the general steps in detail, and our ransomware guide covers the before-during-after of an attack. Both pair well with the public-body rules on this page.

You don't have to build this alone

A big part of the law's spirit is that help is available — much of it free. Here's where to turn.

- **Ohio Auditor of State** — issued guidance (Bulletin 2025-007) and is the office to confirm current specifics with.
- **CyberOhio** — the Ohio Attorney General's initiative with training and resources for local organizations.
- **CISA** (cisa.gov) — free vulnerability scanning of your internet-facing systems, plus guides and [StopRansomware.gov](https://stopransomware.gov).
- **NIST** — the Cybersecurity Framework and small-organization quick-start guides, free to use.
- **FBI IC3** (ic3.gov) — where to report the crime if you're hit.

Our guide on free government cybersecurity help goes into each of these. The point is that a cash-strapped township office can build a real program largely on free, trustworthy resources — cost is not the barrier it might seem.

Following the Auditor of State's guidance

The Auditor of State hasn't just set a deadline — they've published guidance to help you comply. Use it.

The Auditor of State issued Bulletin 2025-007 to help subdivisions understand what's expected. Bulletins like this are written for local officials, not lawyers, and they're a far friendlier read than the statute itself. They're also the most reliable place to catch any updates to the requirements.

Because guidance can be refreshed over time, don't rely on a printout from last year. When you sit down to adopt or review your program, check with the Auditor of State's office for the **current** bulletin and any newer direction. That's the single best way to be sure you're working from today's rules.

✓ Make the bulletin part of your board packet

When your board adopts the program, include the current Auditor of State guidance in the packet and note it in the minutes. It shows the decision was informed, and it gives future officials a clear trail to follow.

The people part: training your staff

The best-written program in the world still runs on the people who answer the phones and open the email.

Ohio has for some time tied in security-awareness training for local-government employees, and it fits naturally with the program the new law wants. Most incidents start with a convincing email or a stolen password, so teaching your team to slow down and spot a scam is among the highest-value things you can do — and it's cheap.

Keep it simple and regular: short refreshers on spotting phishing, a firm rule to verify any payment-change request by calling a known number, and permission for anyone to pause and ask before clicking. Keep a record of who was trained and when — that documentation is part of a real program.

★ I can run a plain-English session for your team

A short, friendly training session — no jargon, real examples your staff will actually remember — goes a long way. I'm glad to come to your office and walk everyone through it. Call (330) 200-8042.

Keeping the records that prove you complied

For a public body, documentation isn't just good practice — it's what an auditor and the public can see.

Keep a clear, dated record of the important steps: the board's adoption of the program (in the minutes), the current program document itself, your training logs, and — if an incident ever happens — a timeline of when you discovered it and when you filed each report. These records show you took the law seriously and acted on time.

Store them where a cyber-incident can't wipe them out — not only on the systems that might be attacked. A backed-up copy plus a printout in the office files is plenty. When you update the program, keep the old versions so there's a trail of your ongoing effort.

✓ Adoption belongs in the minutes

Because the board must formally adopt the program, the single most important record is the meeting minutes showing that vote. Make sure it's clearly recorded, dated, and easy to find.

The slip-ups that trip up public offices

Most compliance gaps I see come down to a short list. Here's what to watch for.

- **Buying software and calling it a program** — the law wants a full, adopted program, not one tool.
- **Never formally adopting it** — a draft in a drawer isn't adopted until the board votes it in.
- **Missing the 7-day report** because nobody knew where to send it.
- **Forgetting the 30-day Auditor report** once the crisis cooled off.
- **Paying a ransom without the required board vote** — a serious misstep under this law.
- **Letting the program and training go stale** after year one.

! The reporting clocks are the easiest thing to miss

In the chaos of an incident, the two deadlines are what slip. Bake them into your written incident plan now — 7 days to Homeland Security, 30 days to the Auditor of State — so they happen automatically, not from memory.

Getting the budget and the board on board

A real program needs a little money and a lot of buy-in. Here's how to make the case without drama.

The honest pitch to a board is simple: this is now the law, the deadlines are tight, and an incident costs far more — in money, downtime, and public trust — than the modest prevention does. Point out how much solid help is free (CISA, CyberOhio, NIST), so the ask is mostly time and a small budget, not a fortune.

It also helps to frame the program as protecting the people the office serves — residents' records, public funds, the services they rely on. Framed that way, adopting a cybersecurity program isn't red tape; it's part of the office's basic duty of care, same as locking the building at night.

✓ Lead with the free help

Boards relax when they hear most of the heavy lifting — frameworks, scanning, training materials — is available at no cost from CISA, CyberOhio, and NIST. The budget conversation gets a lot shorter.

Keeping the program alive year after year

Adopting the program is the start, not the finish. A living program is what actually protects the office.

Put a yearly review on the calendar: re-read the program, update anything that's changed, re-confirm MFA and backups are still working, refresh staff training, and check with the Auditor of State for any updated guidance. Then bring it back to the board to re-affirm, and note it in the minutes.

Elections and staff turnover are a real risk for small offices — knowledge walks out the door. A written, adopted, regularly reviewed program survives those changes, so a new clerk or a new board isn't starting from zero. That continuity is one of the quiet benefits of doing this right.

★ Make me your yearly tune-up

A short annual visit to re-check the settings, confirm backups restore, and help refresh the program keeps everything current through staff and board changes. Call (330) 200-8042 to set up a standing check-in.

Why this is good for the office, not just required

Set aside the mandate for a moment — the program earns its keep regardless.

Local offices are real targets. Attackers know small public bodies often run lean, with older equipment and stretched staff, and they hold exactly the kind of records and payment systems crooks want. A ransomware hit can freeze payroll, utilities billing, and public records for weeks. The program is how you avoid that nightmare, not just a box to check.

And the same preparation that satisfies the law also speeds your recovery if something slips through, smooths any cyber-insurance you carry, and reassures the residents you serve that their information is in careful hands. One effort, many payoffs.

✓ Compliance and real safety point the same way

This is one of those happy cases where doing what the law asks and doing what actually protects you are the very same work. Build the program well once and you get both.

A simple game plan to get compliant

Here's a calm order of operations to go from 'we should do this' to 'we've adopted it.'

- ❑ **Step 1:** confirm with counsel and the Auditor of State that the law applies to you and get the current guidance.
- ❑ **Step 2:** turn on the technical baseline — MFA, tested backups, updates, individual logins.
- ❑ **Step 3:** draft a right-sized program using a free framework and the state and federal resources.
- ❑ **Step 4:** write the incident plan with both reporting clocks and the ransom-vote rule built in.
- ❑ **Step 5:** have the board formally adopt the program, recorded in the minutes.
- ❑ **Step 6:** train the team, keep the records, and set a yearly review.

Six steps, most of them using free help, and your office goes from exposed and non-compliant to prepared and on the record. Take them in order and it's far less daunting than it looks from the outside.

Common Questions

The questions local officials ask me most about the new rules, answered plainly. Remember: general information, not legal advice.

Q: Does this really apply to a tiny township with two staff?

If you're a political subdivision — a township, village, or county office — you should assume it applies and confirm with your counsel. Size doesn't exempt you, but your program can be lean and built largely on free help.

Q: What exactly are the reporting deadlines?

After a cybersecurity or ransomware incident, report to Ohio Homeland Security as soon as possible and no later than 7 days after discovery, and to the Ohio Auditor of State as soon as possible and no later than 30 days. Both clocks start when you discover it.

Q: Can our office just pay the ransom to get back up fast?

Not on your own. The law says a subdivision shall not pay unless its legislative authority formally approves it by resolution or ordinance explaining why it's in the public's best interest. Build that vote into your incident plan.

Q: We have almost no budget. How are we supposed to do this?

Much of what you need is free — frameworks from NIST, scanning and guides from CISA, training and resources from CyberOhio. The main ask is time and a modest budget, and a lean program still counts.

Q: Do schools have to do this too?

Schools and districts should confirm their exact status and any overlapping education rules with their counsel and the Auditor of State, rather than assume either way. Don't guess — ask.

★ Need a hand getting your office compliant?

I help small Ohio public offices turn on the protections, build the program, and get ready to report fast. Plain English, patient pace, no upsell. 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 public-body cybersecurity rules 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 Law's Three Parts

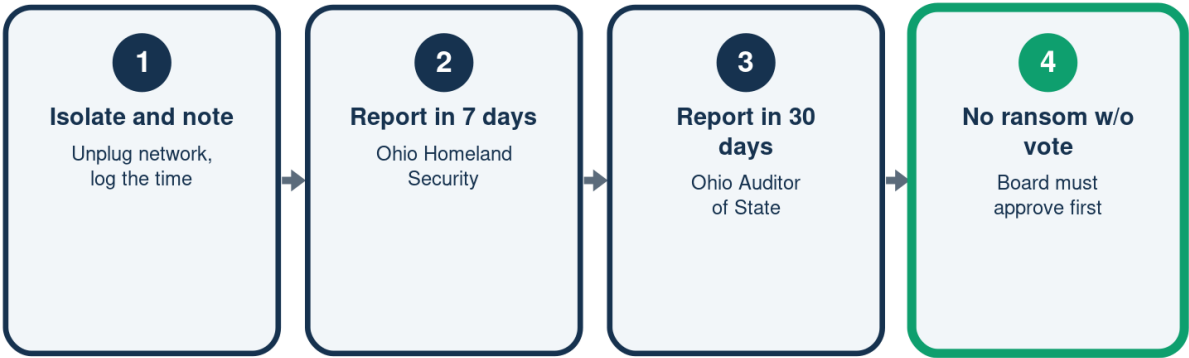
What ORC 9.64 asks of a public body

	Part	What it means
Adopt a program	Board votes it	onto the record
Report incidents	7 days / 30 days	two offices
Ransom rule	No pay without	a board vote

Confirm current specifics with counsel and the Auditor of State.

When an Incident Hits

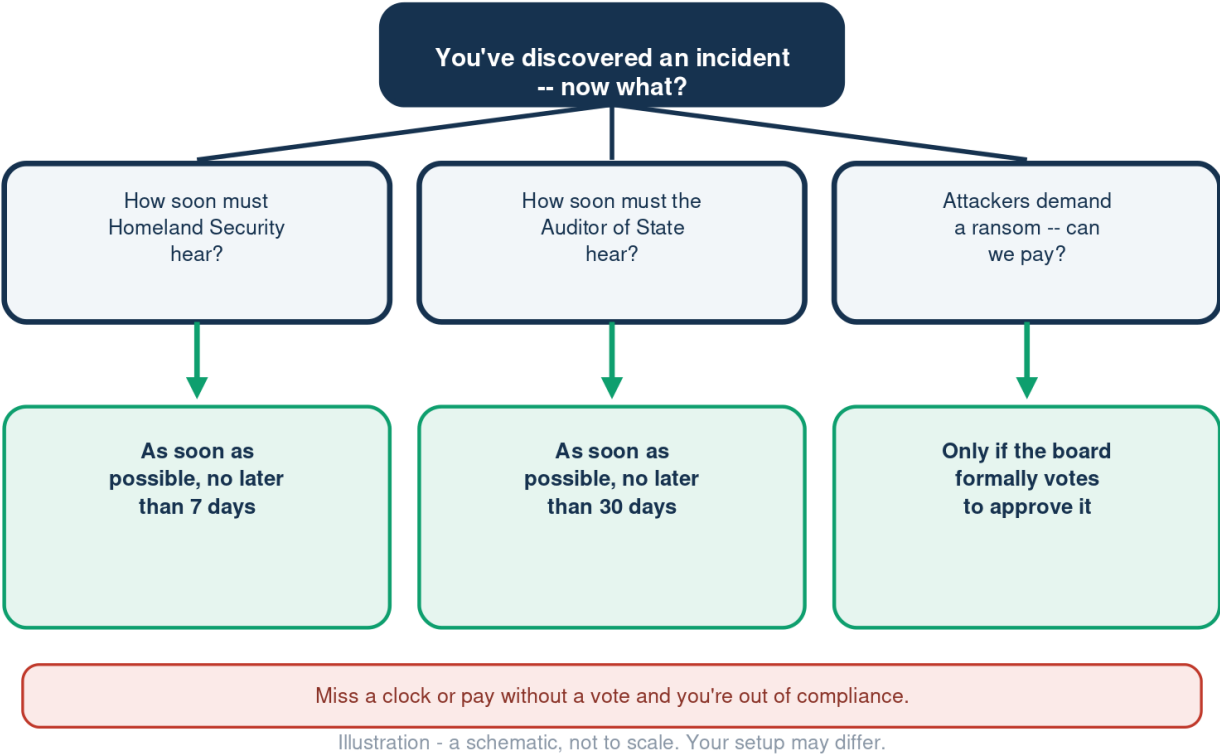
The order that keeps you compliant



Both clocks start at discovery -- bake them into your incident plan.

Who Do You Report To?

After a cybersecurity or ransomware incident



Free Help You Can Lean On

Cost shouldn't be the blocker

	Resource	What you get
Auditor of State	Guidance	Current rules
CyberOhio	Training	Resources
CISA	Free scanning	Guides
NIST	Frameworks	Quick-starts

A lean office can build a real program mostly on free resources.



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