



An Extended Guide · No. 2074

A Customer-Data Breach in Ohio: Who You Must Tell and When

Ohio's notification rules in plain
English — and when to call a lawyer

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. If a breach does happen, Ohio law can require you to tell the people whose information was exposed — so knowing the rules ahead of time keeps a bad day from becoming a legal one.

If customer data gets out, who do you have to tell?

It's the question that keeps an owner up at night after a break-in: do I have to tell my customers, and when? Ohio has a law that answers it. This guide walks through it in plain English so you know what the rules ask — and when to pick up the phone to a lawyer.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. I've spent 30-plus years helping small businesses with their technology in plain language. I'm a tech helper, not a lawyer — so I'll explain the shape of the rules and help you prepare, but the judgment calls in a real breach belong with an attorney and your insurer.

Here's the reassuring part: this is far easier to handle if you've read about it **before** anything goes wrong. An owner who already knows the 45-day clock exists, and who to call first, handles a breach calmly. An owner learning it mid-crisis does not. Let's get you in the first group.

★ Let's set up your 'what-if' plan now, while it's calm

The best time to think about a breach is when you're not having one. I can help you write down who to call, where your customer data lives, and what you'd need in a hurry — so a crisis becomes a checklist. 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 breach-notification rules.

- ❑ Ohio's breach-notification law lives in **ORC 1349.19** and covers computerized **personal information** about Ohio residents.
- ❑ 'Personal information' means a **name plus** a sensitive data element — an SSN, driver's license/state ID number, or a financial account or card number with its access code — when not encrypted or redacted.
- ❑ The trigger is unauthorized **access and acquisition** that causes, or likely causes, a material risk of identity theft or fraud.
- ❑ You must notify affected residents **as quickly as possible, no later than 45 days** after you discover it.
- ❑ If one breach hits **more than 1,000** Ohio residents, you must also notify the nationwide **credit bureaus**.
- ❑ The **Ohio Attorney General** can investigate and bring a civil action — and whether a breach is even notifiable is a legal call. Call a lawyer early.

! Call your lawyer and insurer before you send anything

Whether you must notify, and exactly what the notice must say, is a legal judgment with real consequences. Don't guess and don't rush out a letter on your own — loop in an attorney and your cyber-insurer first. The 45-day clock gives you room to do this right.

Why Ohio makes you tell people

Understanding the point of the law makes the rules easier to follow.

When someone's Social Security number or bank details slip out, the danger isn't over — it's just beginning. A crook can open accounts, file fake tax returns, or drain money for months. The faster the person knows, the faster they can freeze credit, watch their accounts, and protect themselves.

So Ohio's law, in section 1349.19 of the Revised Code, requires businesses that hold this kind of information to warn the people affected when it's been exposed. It's not meant to punish you for being a victim of a crime — it's meant to give the next potential victims a fighting chance.

That framing helps when a breach feels unfair. Notifying isn't an admission that you did something wrong; it's the responsible, legally required step that protects the people who trusted you with their data.

! 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 law even apply to me?

The law reaches a lot further than most owners expect, so it's worth a careful look.

The law applies to anyone who owns or licenses computerized personal information about Ohio residents. That's broad on purpose. You don't have to be a big company or a tech business. If you keep customer records on a computer that include the sensitive details we'll describe next, you're likely in scope.

Think about who that catches: a tax preparer, an auto shop that finances cars, a landlord with tenant applications, a clinic, a contractor who ran credit checks, a shop that stores card numbers. If Ohio residents' sensitive data sits on your systems, this law is talking to you.

✓ It's about the data, not your industry

Don't assume you're exempt because you're 'not a tech company.' The question is simply whether you hold Ohio residents' personal information on a computer. Most small businesses that keep customer records do.

What 'personal information' actually means

This is the heart of the law. Not every piece of customer data triggers it — the definition is specific.

Under the law, 'personal information' means a person's **name** combined with at least one of these sensitive data elements, when that element isn't encrypted or redacted:

- A **Social Security number**.
- A **driver's license number** or state ID number.
- A **financial account number, or credit/debit card number**, together with any security code, access code, or password that would let someone use the account.

The 'name plus' part matters. A loose list of email addresses, or card numbers with no name and no access code, may not meet the definition. And if the sensitive element was properly **encrypted or redacted**, the law generally treats it as not exposed. This is exactly the kind of line a lawyer helps you read correctly.

✓ Encryption can keep a loss from becoming a breach

If a stolen laptop's drive was encrypted, the data on it is generally unreadable — which can mean no notifiable breach. That's one more reason our guides push BitLocker and FileVault: encryption isn't just protection, it can change your legal exposure.

When an incident becomes a notifiable breach

Not every scare is a breach under the law. Two things generally have to be true before the clock starts.

Access AND acquisition

The law looks for unauthorized **access and acquisition** of the data — not just that someone might have been able to reach it, but that the information was actually gotten. A thief who grabbed the files is different from a glitch that briefly exposed a screen nobody saw.

A material risk of harm

There also has to be a real — 'material' — risk that the exposure causes identity theft or other fraud, or a reasonable belief that it will. If the data was encrypted and stays unreadable, that risk may not exist.

! Whether it's 'notifiable' is a legal judgment — not yours alone

These words — access, acquisition, material risk — carry legal weight, and guessing wrong in either direction is costly. Over-notify and you alarm people needlessly; under-notify and you break the law. This is precisely why you call a lawyer and your insurer before deciding.

The 45-day clock — and when it can pause

Once you've determined a breach is notifiable, the timing rule is the one number to burn into memory.

You must notify the affected Ohio residents in the **most expedient time possible, and no later than 45 days** after you discover the breach. 'Most expedient time possible' matters as much as the 45 days — you're expected to move promptly, not to sit on it for 44 days out of habit.

The law does allow the clock to pause in two situations: when law enforcement tells you notice would interfere with a criminal investigation, or while you take reasonable steps to figure out the scope of the breach and restore your systems. Those pauses are legitimate — but they're judgment calls your lawyer should bless, not excuses to delay.

✓ Write down the date you discovered it

The clock starts at discovery, so the moment you realize something happened, note the date and time. That single fact anchors every deadline that follows, and your lawyer and insurer will ask for it first.

The big-breach rule: more than 1,000 residents

There's a second notification that kicks in only when a breach is large, and it's easy to forget.

If a single breach affects **more than 1,000 Ohio residents**, you must also notify the nationwide consumer reporting agencies — the credit bureaus — about the timing, distribution, and content of the notices you're sending to residents. This lets the bureaus brace for a wave of people checking and freezing their credit.

For a lot of small businesses, you'll never cross 1,000 affected Ohio residents in one breach, so this won't apply. But if you hold a big customer list — a busy clinic, a property manager, a shop with years of card records — it absolutely can, and it's exactly the kind of detail a lawyer makes sure you don't miss.

✓ Know your numbers before you're asked

Have a rough sense of how many customer records you hold and how many are Ohio residents. When a breach happens, that count drives which notifications you owe — and you don't want to be guessing under pressure.

What notification looks like for your situation

The law is the same for everyone, but the practical weight of a breach depends a lot on how much sensitive data you hold and how many people it touches.

If you hold a little sensitive data

A solo shop or small office with a modest customer list still has duties, but a breach is more manageable: fewer people to notify and far less chance of crossing the 1,000-resident credit-bureau line.

- Know exactly where the sensitive data lives — which files hold names plus SSNs, IDs, or card details.
- Encrypt those files and devices; encryption can keep a loss from becoming a notifiable breach.
- Keep a short contact list: your lawyer, your insurer's hotline, your IT help.
- You likely stay well under 1,000 Ohio residents, so the credit-bureau step may never apply — but confirm with your lawyer.

If you hold lots of customer records

A clinic, property manager, or shop with years of records faces a bigger job: more residents to notify, a real chance of the 1,000-resident rule, and closer attention from regulators.

- Map your data now — how many records, how many Ohio residents, what sensitive elements.
- Assume the 1,000-resident credit-bureau notification could apply, and plan for it.
- Line up an attorney and your insurer in advance so a large breach doesn't catch you cold.
- Watch for overlapping rules if you handle medical or financial data — your lawyer confirms which apply.

★ Not sure how much sensitive data you're sitting on?

I can help you find and map where the sensitive records live, count roughly how many you hold, and get them encrypted — so you'd know your exposure fast if a breach ever hit. Call (330) 200-8042.

The first calls: lawyer and insurer, not a letter

The instinct after a breach is to rush out an apology to customers. Resist it. The right first move is to call the professionals.

Your cyber-insurance policy almost certainly wants you to call its incident hotline first — they direct the response and bring in the forensics and legal team, often at no extra cost to you. Our cyber-insurance application and coverage guides explain why that call comes before nearly everything else. Our guide 'The First Hour After a Hack' walks the full order of steps.

A lawyer who knows breach law will then help you decide the hardest questions: is this even notifiable, who exactly must be told, what the notice has to say, and whether any pause in the clock applies. Getting those right is worth far more than getting a letter out a day sooner.

! A wrong or early notice can make things worse

A notice that admits the wrong things, goes to the wrong people, or leaves out what the law requires can create new legal problems on top of the breach. Let the professionals shape it. The 45-day window exists so you can do this carefully.

How the notice typically goes out

When you do notify residents, there are a few common, lawful ways to do it. Your attorney confirms which fits your situation.

- **Written notice** mailed to the person's last known address.
- **Electronic notice**, where that's consistent with how you normally deal with the person and with the applicable rules.
- **Telephone notice** in some circumstances.
- **Substitute notice** — for example a website posting and media notice — which the law allows in limited situations, such as when the cost or the number of people makes direct notice impractical.

The method matters less than the content and the timing, both of which your lawyer should guide. The goal throughout is simple and human: give the affected person enough clear information to protect themselves quickly.

✓ Plain, honest, and helpful beats legalistic

The best breach notices tell people clearly what happened, what information was involved, and exactly what they should do now — freeze credit, watch accounts, change passwords. Your lawyer handles the required legal pieces; you make sure it's readable.

The Ohio Attorney General's role

It helps to know who's watching, so you take the rules as seriously as they deserve.

The Ohio Attorney General's office investigates breach-notification matters and can bring a civil action against a business that doesn't follow the law. That's the real teeth behind the rules — the reason 'we meant to get around to it' isn't a safe plan.

The flip side is encouraging: the Attorney General's office also runs CyberOhio, an initiative with free training and resources to help small businesses protect themselves in the first place. The state would much rather help you avoid a breach than pursue you after one. Our guide on free government help points you to those resources.

✓ Good-faith effort shows

A business that clearly took reasonable security seriously and handled a breach responsibly is in a very different position from one that ignored both. Our Ohio safe-harbor guide explains how a written program can even become a legal defense.

Watch for overlapping rules

Ohio's breach law isn't always the only one that applies, and the others can have their own deadlines and audiences.

Depending on your business, other rules may stack on top of ORC 1349.19. Health information can bring HIPAA requirements into play. Financial businesses and tax preparers may owe notice under the federal FTC Safeguards Rule. Card data brings PCI obligations from the card brands. Some of these have different thresholds and shorter clocks.

You don't need to untangle this yourself — that's the lawyer's job. But you should go in knowing that 'who must I tell' can have more than one answer, and that the strictest rule often sets the pace. Our FTC Safeguards guide covers that federal 30-day notification for financial businesses.

! One breach can trigger several laws at once

A single incident at a tax office could invoke Ohio's law, the FTC Safeguards Rule, and IRS notification expectations together. That's not a reason to panic — it's a reason to let one attorney coordinate all of it instead of answering each piece piecemeal.

The prep that makes a breach survivable

Almost everything that makes a breach go smoothly is done long before the breach. Here's your calm-day checklist.

- ❑ Know **where your sensitive data lives** — which systems and files hold names plus SSNs, IDs, or card details.
- ❑ **Encrypt** those devices and files — it protects data and can change whether a loss is even notifiable.
- ❑ Keep a **contact card**: your cyber-insurer's hotline, a breach lawyer, and your IT help.
- ❑ Know roughly **how many Ohio residents** you hold data on, for the 1,000-resident question.
- ❑ Keep **tested backups** so you can restore and prove what was affected.
- ❑ Write a one-page plan for **who does what** in the first hours — see our 'First Hour After a Hack' guide.

None of that is expensive or hard. It's the difference between a breach that's handled in a few organized days and one that spirals because nobody knew where to start.

Write down what you did, as you do it

During and after a breach, a running record is one of your most valuable protections.

From the moment you discover a possible breach, keep a dated log: when you found it, who you called, what you learned, and what you decided and why. If the Attorney General ever asks whether you acted reasonably and on time, that log is your answer — it turns a blur of stressful days into a clear, defensible timeline.

Keep the records somewhere a crisis can't erase — not only on the systems that might be compromised. A simple dated document, backed up and printed, is plenty. Your lawyer will thank you for it.

✓ The timeline is the story

If a question ever arises, what matters is whether you moved promptly and reasonably. A clear, dated record showing you discovered the breach, called the pros, and notified within the window tells that story far better than memory ever could.

The mistakes that turn a breach into a bigger problem

Most breach missteps I read about fall into a short, avoidable list. Now you'll see them coming.

- **Deciding on your own** whether it's notifiable, instead of asking a lawyer and your insurer.
- **Sending a notice too fast**, before you know the scope — or **sitting on it** past the 45-day clock.
- **Forgetting the 1,000-resident credit-bureau step** on a large breach.
- **Powering off or wiping machines** before forensics can see them (see our ransomware and first-hour guides).
- **Not writing anything down**, leaving no timeline to show you acted reasonably.
- **Ignoring overlapping rules** like HIPAA, FTC Safeguards, or PCI.

! Silence is the most dangerous choice

Hoping a breach stays quiet is how a manageable problem becomes a legal one. The law, your insurer, and your customers all respond far better to prompt, honest handling than to a cover-up that surfaces later.

Taking care of the people, not just the paperwork

Behind every notice is a person who trusted you with their information. How you treat them matters — for them and for your business.

A breach is frightening to receive news about. The businesses that come through with their reputations intact are the ones that are honest, clear, and genuinely helpful — explaining plainly what happened and what the person should do, maybe offering credit monitoring, and answering questions patiently.

Your customers generally understand that crime happens. What they remember is whether you had their back when it did. Handled well, even a breach can leave people feeling you took their trust seriously.

★ I'll help you be ready to be the good guy

Being able to respond fast and clearly starts with knowing your own systems and data cold. I can help you get there now, so if the worst happens you can focus on your customers instead of scrambling. Call (330) 200-8042.

The best notification is the one you never send

All of this is a lot easier to avoid than to handle. The same basic controls that stop most breaches are the ones we recommend everywhere.

- **MFA everywhere** — most breaches start with a stolen password; a second sign-in step stops them.
- **Encryption** on laptops and sensitive files — so a lost device isn't a reportable breach.
- **Tested backups**, kept offline, so an attack can't erase your proof or your business.
- **Current updates** and end-of-support software replaced.
- **Careful email habits** and a call-back rule for payment changes — see our payment-fraud guide.

Do these and you dramatically cut the odds of ever needing this guide for real. Our Microsoft 365, Google Workspace, and backup fire-drill guides walk through each one at a kitchen-table pace.

How cyber insurance fits into all this

A good cyber policy is built for exactly this moment, and it changes how a breach plays out.

Many cyber policies cover the real costs of a notifiable breach: the forensics to find out what happened, legal help to decide who must be told, the cost of printing and mailing notices, and credit monitoring for affected people. That's why the policy wants you to call its hotline first — it's coordinating and paying for the very response this guide describes.

If you don't have cyber insurance yet, the cost of a single notifiable breach — lawyers, mailings, monitoring, lost time — is a sobering argument for getting a quote. Our cyber-insurance guides cover what a policy pays for and how to fill out the application honestly.

✓ Find your hotline number before you need it

Write your insurer's incident hotline and policy number somewhere you can reach even if your computers are down. The worst time to go hunting for it is in the middle of the emergency it's meant for.

A one-page breach plan you can actually use

Pull it all together into something a stressed person could follow without thinking too hard.

- ❑ **Step 1 — Contain, don't destroy:** isolate affected machines from the network, but don't power them off or wipe them.
- ❑ **Step 2 — Call your insurer's hotline** and note the date and time you discovered it.
- ❑ **Step 3 — Call a breach lawyer** to decide if it's notifiable and who must be told.
- ❑ **Step 4 — Report the crime** to the FBI at ic3.gov if advised.
- ❑ **Step 5 — Notify affected residents** within the window, and the credit bureaus if over 1,000.
- ❑ **Step 6 — Keep a dated log** of everything, and fix what let it happen.

Print this, tape it inside a drawer, and tell your team it's there. A breach will never feel calm, but a plan on paper turns panic into a list you can work through one line at a time.

Common Questions

The questions owners ask me most about Ohio's breach-notification rules, answered plainly. Remember: general information, not legal advice.

Q: A laptop was stolen but the drive was encrypted. Is that a breach?

Often not a notifiable one — if the sensitive data was properly encrypted and stays unreadable, the law generally treats it as not exposed. But confirm with a lawyer, because the details matter. It's one more reason to encrypt every device.

Q: How fast do I really have to tell people?

As quickly as possible, and no later than 45 days after you discover the breach. The clock can pause for a law-enforcement investigation or while you determine scope and restore systems, but those are judgment calls for your lawyer.

Q: Do I have to tell the credit bureaus too?

Only if a single breach affects more than 1,000 Ohio residents — then you also notify the nationwide credit bureaus about the notices you're sending. Below that, this step usually doesn't apply.

Q: Who decides whether something even counts as a breach?

Legally, that's a judgment — so you and your attorney decide together, with your insurer's incident team. The test looks at whether data was actually accessed and acquired and whether there's a material risk of identity theft or fraud.

Q: What happens if I just don't notify?

The Ohio Attorney General can investigate and bring a civil action. Beyond the legal risk, failing to notify breaks trust with your customers. Prompt, honest handling is always the safer path.

★ Worried you might be sitting on a breach right now?

Call me and your insurer's hotline right away — don't wait and don't start deleting things. I'll help you figure out what happened and preserve what the pros need. 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 an Ohio customer-data breach 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 Counts as Personal Info

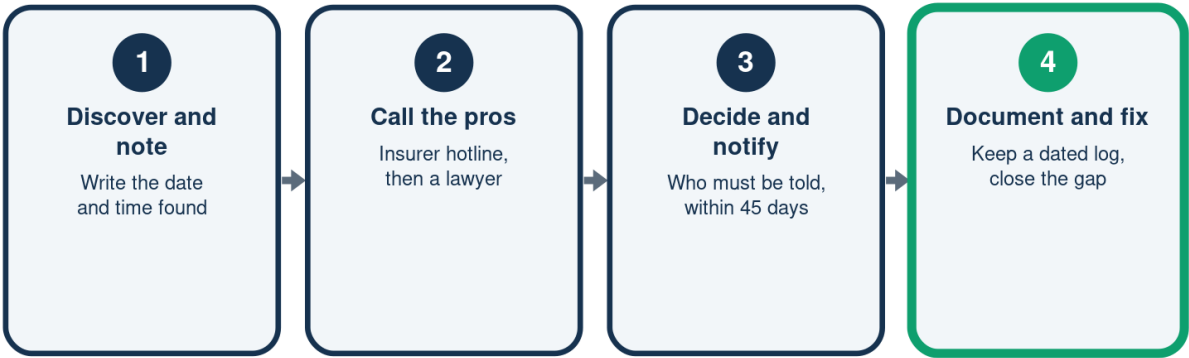
Name PLUS a sensitive element -- unless encrypted

Data you hold		Covered?
Name + SSN	Yes	Covered
Name + license no.	Yes	Covered
Name + card + code	Yes	Covered
Encrypted/redacted	Generally not	Usually safe

A lawyer confirms the line -- 'name plus' and encryption both matter.

The Breach Timeline

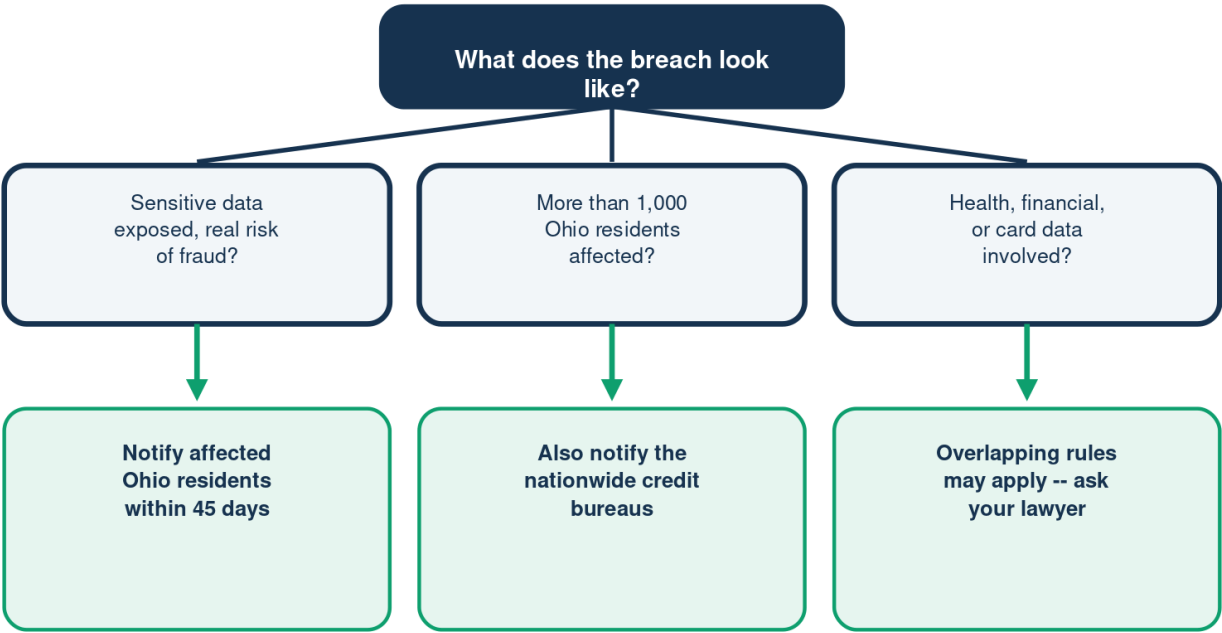
What happens after you discover it



The 45-day window exists so you can do this carefully, not alone.

Who Do You Have to Tell?

Let the facts point the way



Whether a breach is notifiable is a legal call -- confirm it, don't guess.

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

First Moves After a Breach

Do these, skip those

	Do	Don't
The machines	Isolate them	Power off/wipe
First call	Insurer hotline	Customer letter
The decision	Ask a lawyer	Decide alone
The record	Log everything	Rely on memory

Preserve evidence and call the pros before you notify anyone.



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