



An Extended Guide · No. 2076

The First Hour After a Hack: Who to Call and What Not to Touch

A calm, correct order of steps that
protects your evidence and your business

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. And if the worst does happen, the first hour matters most: a few calm, correct moves protect your evidence, your coverage, and your chance to recover.

The first hour after a hack: a calm plan

The moment you realize you've been hacked, your heart races and every instinct screams to do something — unplug, delete, reboot, start cleaning up. This guide gives you the opposite: a short, calm order of steps that protects your business when it matters most.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. I've spent 30-plus years helping small businesses through their worst computer days. The single best thing you can do about a hack is read this before one ever happens — because in the moment, you won't have time to figure it out.

Here's the whole idea in one breath: don't panic, don't destroy anything, and make a few phone calls in the right order. The owners who come through a breach in good shape aren't the ones who move fastest — they're the ones who move correctly. That's completely learnable, and that's what this guide teaches.

★ Program my number in before you ever need it

If you think you've been hit, you can call me and I'll help you take the right first steps — what to unplug, what to leave alone, who else to call. Save my number now so it's there in the panic. Call or text me at (330) 200-8042.

The whole guide, on one page

If you remember only these things, you'll handle the first hour better than most.

- ❑ **Stay calm.** The first hour is about not making it worse, not about fixing it instantly.
- ❑ **Isolate, don't destroy.** Disconnect affected machines from the network — but do NOT power them off or wipe them.
- ❑ **Call your cyber-insurance hotline FIRST.** They direct the response and bring in the forensics and legal team.
- ❑ **Then call your IT help** (like me), then **law enforcement** — the FBI at ic3.gov.
- ❑ **Change passwords from a clean device**, not the one that may be compromised.
- ❑ **Don't 'clean up'** or delete anything until the experts tell you to — you could be destroying the evidence they need.

! The urge to 'fix it fast' is the dangerous one

Powering off a machine, wiping it, or deleting the bad files feels like taking control — but it can erase the evidence your insurer and forensics team need, and it can void your coverage. The right first move is almost always to pause and make the calls.

First: take a breath

It sounds soft, but staying calm is the most practical thing on this whole list. Panic is what causes the costly mistakes.

A hack triggers real fear — about money, about customers, about your reputation. That fear pushes people to act fast and wrong: yanking cords, rebooting, formatting a drive, firing off a panicked email to everyone. Almost every one of those rushed moves makes the situation harder to recover from.

So the very first step is simply to slow down for sixty seconds. The damage is mostly already done; a few careful minutes now won't change that, but a few careless ones can. Remind yourself: your job in this first hour is to **preserve the situation and call the right people**, not to solve the whole thing yourself.

✓ You are not expected to fix this alone

This is exactly the kind of moment where you lean on professionals — your insurer's response team, your IT help, law enforcement. Your job is to not make it worse and to get them involved quickly. That's a job you can do.

How do you even know you've been hacked?

Sometimes it's obvious; sometimes it's a quiet wrongness. Here are the signs that should put you on alert.

- A **ransom message** on screen, or files renamed and unopenable — that's ransomware (see our ransomware guide).
- You're **locked out** of your email or accounts, or passwords suddenly don't work.
- **Customers or vendors** report strange emails 'from you' that you didn't send.
- **Money moved** that shouldn't have — a payment redirected, a wire you didn't authorize (see our payment-fraud guide).
- Your computer is wildly slow, pop-ups appear, or settings changed on their own.
- Your bank, a vendor, or a security service **warns you** of suspicious activity.

If something feels wrong but you're not sure, treat it as real until you've confirmed otherwise — but still follow these calm steps rather than poking around. It's far better to make the calls over a false alarm than to dismiss a real breach.

Isolate the machine — but leave it on

This is the single most important technical move in the first hour, and the one people most often get wrong.

The goal is to stop the problem from spreading while preserving the evidence of what happened. So you want to **cut the affected machine off the network** — unplug the network cable, or turn off its Wi-Fi — so malware can't reach your other computers or phone home. Isolate it.

But do **not** power it off, and do **not** wipe it or reinstall anything. A running machine holds valuable clues in its memory and current state that forensics experts may need to understand the attack — clues that vanish the instant you shut down. Your insurer's team will tell you when it's safe to power down; until then, leave it on but disconnected.

! Unplug from the network, not from the wall

Pull the network cable or switch off Wi-Fi to isolate the machine — yes. Hold the power button or yank the power cord — no, not yet. That one distinction protects both the evidence and, often, your path to recovery.

Preserve the evidence

Everything you can preserve now helps the experts figure out what happened, how bad it is, and how to get you back.

Resist the urge to tidy up. Don't delete suspicious files, don't clear your email, don't reset the machine to 'start fresh.' All of that is evidence — it's how forensics traces what the attacker touched, what data was reached, and whether you have legal notification duties. Destroying it can leave you unable to answer critical questions later.

Do start a simple written log instead: the date and time you noticed, what you saw, what you did and when, and who you called. Take photos of any ransom message or error on screen with your phone. This record is gold for your insurer, your forensics team, and any legal notice you may owe.

✓ Your phone is your evidence camera

Snap a photo of whatever's on the screen — the ransom note, the error, the strange message — before anything changes. It costs nothing, takes five seconds, and can tell the experts a lot about what hit you.

Call your cyber-insurance hotline FIRST

If you remember one phone call from this guide, make it this one. Before IT, before anyone — call your insurer's incident hotline.

Most cyber-insurance policies want you to call their 24-hour incident hotline the moment you suspect a breach, and there's a very good reason. The insurer **directs the response**: they bring in the forensics specialists and the breach lawyers, often at no extra cost to you, and they coordinate the whole recovery. These are experts you couldn't easily find or afford on your own, standing by for exactly this.

Calling them first also protects your coverage. Many policies require you to notify them before you start spending money on outside help or taking major steps — do it out of order and you can jeopardize the claim. Our cyber-insurance application and coverage guides explain how this works and why the hotline matters so much.

! Find the hotline number BEFORE the emergency

The worst time to go hunting for your policy and hotline number is while your systems are down. Write the insurer's incident hotline and your policy number on a card and keep it somewhere that doesn't depend on the computers — a drawer, your wallet, a phone note. Do it today.

Then your IT help, then law enforcement

With your insurer engaged, the next two calls fall into place. Order still matters.

Your IT help

Next, bring in your trusted IT person — someone like me — to work alongside the insurer's team, help contain things safely, and start planning recovery from clean backups. If your insurer's team is handling the technical response, your own IT helper is still valuable for knowing your setup and coordinating.

Law enforcement

Then report the crime. For internet crime, business email compromise, and wire fraud, the place to go is the **FBI's IC3 at ic3.gov**. Reporting creates an official record, can help recover redirected money if you act fast, and feeds the bigger fight against these crooks. Your insurer or lawyer will advise on timing and what to include.

✓ Let the insurer quarterback

Once your insurer's incident team is engaged, follow their lead on the order and timing of the other calls. They do this every day and will make sure nothing important — including legal notification duties — gets missed.

What the first hour looks like for your setup

The steps are the same for everyone, but whether you have cyber insurance and staff changes how the first hour actually plays out.

If you have cyber insurance

Your first hour is mostly about preservation and one phone call. The insurer's team takes the wheel on the technical and legal response, so your job is to not make things worse and to get them on the line fast.

- Isolate affected machines from the network, but leave them on.
- Grab your hotline card and call the insurer's incident line right away.
- Start your written log and photograph anything on screen.
- Follow the insurer team's instructions from there — they coordinate the rest.

If you don't have cyber insurance yet

Without an insurer's hotline, you're coordinating the response yourself, so lean harder on trusted IT help and free government resources — and consider getting a policy once you're through this.

- Isolate and preserve exactly the same way — don't power off or wipe.
- Call a trusted IT professional (like me) as your first call instead.
- Report to the FBI at ic3.gov, and use CISA's free resources at cisa.gov.
- Afterward, read our cyber-insurance guides — a policy makes the next incident far less lonely.

★ No insurer hotline to call? Call me.

If you don't have a cyber policy and you think you've been hit, I'll help you take the right first steps and bring in whatever extra help you need. And once you're recovered, I'll help you get set up so the next scare is far less scary. Call (330) 200-8042.

Change passwords — from a clean device

Changing passwords is important, but how and where you do it decides whether it actually helps.

If an attacker is in your accounts, you'll want to lock them out by changing passwords — especially on email, which is the master key to everything else. But if you change them from the **same computer that may be compromised**, the attacker's software can simply capture the new ones. You'd be handing them the fresh keys.

So use a **clean device** the attacker hasn't touched — your phone on cellular data, or a different computer — to change the critical passwords. Start with email, then anything that uses that email to reset. And turn on MFA everywhere while you're at it, so a stolen password alone can't get back in. Our Microsoft 365 and Google Workspace guides show how.

! Email first, from a device you trust

Your email is the reset point for most other accounts, so securing it comes first — and always from a device you're confident is clean. Coordinate with your insurer's team, since in some cases they'll want to preserve things before you start changing credentials.

Don't 'clean it up' until you're told to

The instinct to scrub the machine and get back to normal is strong. It's also the instinct most likely to cost you.

After the shock wears off, there's huge temptation to reinstall Windows, delete the bad files, restore everything, and move on — to make the bad day disappear. But until the forensics team has looked, that cleanup destroys evidence of what the attacker did and what data they reached. That evidence is what tells you whether you have legal duties to notify customers.

It can also backfire technically: restore too soon and you might bring the infection right back, or overwrite the very backup you need. Let the experts confirm the attacker is truly out and tell you the safe order to rebuild. Patience here is not weakness — it's what a clean recovery requires.

! Premature cleanup can create legal problems

If a breach exposed customer data, you may have notification duties under laws like Ohio's breach-notification rule — and you can't assess that if you've already wiped the evidence. Our Ohio breach-notification guide explains why preserving the scene protects you legally, not just technically.

Who else might need to know

Beyond the core calls, a breach can ripple outward. Your insurer and lawyer guide this, but here's the landscape.

- **Affected customers** — if their personal data was exposed, you may be legally required to notify them (see our Ohio breach guide).
- **Your bank** — immediately, if money was moved or account details were exposed; fast action can sometimes recover funds.
- **Staff** — so they stop using compromised systems and watch for follow-on scams aimed at them.
- **Vendors and partners** connected to your systems, so the attack doesn't spread to them.
- **Regulators** — depending on your industry (health, financial, card data), extra rules and deadlines may apply.

You don't have to figure out all of this in the first hour. Preserve, call your insurer, and let their legal team map out exactly who must be told and by when. The first hour is about setting that up correctly.

Build your emergency contact card now

Everything in this guide depends on having a few numbers at your fingertips. Let's build that card today, while it's calm.

- ❑ Your **cyber-insurer's 24-hour incident hotline** and your policy number.
- ❑ Your **IT helper's** number (mine is on the back page).
- ❑ Your **bank's** fraud line.
- ❑ The FBI **IC3** web address: ic3.gov.
- ❑ A note: **isolate, don't power off; don't delete anything; call the insurer first.**
- ❑ Where your **backups** are and how to reach them.

Print it, keep a copy somewhere that doesn't rely on your computers — a drawer, a wallet, a printed sheet by the main workstation — and make sure whoever might be first to notice knows where it is. A card on paper works even when every screen in the building is locked.

The 'do not' list, all in one place

Sometimes it's clearer to name the mistakes directly. In the first hour, do not do any of these.

- **Don't power off or restart** the affected machine — isolate it instead.
- **Don't wipe, reinstall, or factory-reset** anything.
- **Don't delete** suspicious files, emails, or logs.
- **Don't pay** a ransom on your own impulse — involve your insurer and law enforcement first (see our ransomware guide).
- **Don't keep using** the compromised accounts or machine as if nothing happened.
- **Don't stay silent** and hope it blows over — the clock on legal duties may already be running.

! When in doubt, do nothing and make the call

If you're unsure whether an action is safe, the answer in the first hour is almost always to leave it alone and call your insurer or me. Inaction preserves your options; a wrong action can close them for good.

What comes after the first hour

Once you've preserved the scene and made the calls, the response settles into a longer, calmer rhythm — led by the experts.

The forensics team investigates what happened and what was reached. Your lawyer determines any notification duties. Together with your IT help, you plan recovery: confirming the attacker is out, rebuilding clean systems, and restoring from backups you've verified are safe. It takes longer than you'd like, but done right, it's done once.

This is where tested backups earn their keep — restoring from a good backup is often the fastest clean way back. If you've never tested a restore, you may not know your backup works until this exact moment. Our backup fire-drill guide makes sure you never learn that the hard way.

✓ Recovery is a marathon, not the first hour's sprint

Give yourself and your team grace. A proper recovery can take days. The first hour's job was to protect your options; the days after are about using them well, with the experts leading.

Learn from it and close the door

Once you're back on your feet, a little honest reflection turns a bad experience into a much safer business.

With the experts' findings in hand, you'll usually know how they got in — a stolen password, a clicked link, an unpatched machine. That's not a moment for blame; it's a map. Close that specific door, and look for the other doors like it. Most attacks come through a handful of ordinary gaps.

- Turn on **MFA everywhere** if it wasn't already — the top defense against stolen passwords.
- Get **updates current** and replace end-of-support software.
- Confirm your **backups are offline and tested**.
- Refresh **staff training** on spotting scam emails.
- Review **who has access** to what, and cut what's unused.

Our Microsoft 365, Google Workspace, backup fire-drill, and payment-fraud guides each tackle one of these. Pick the gap that let this one in, and start there.

A quick word if it's ransomware

Ransomware has its own wrinkles, so here's how the first hour differs — with more detail in our dedicated guide.

If you're staring at a ransom demand, the first-hour rules still hold: stay calm, isolate the machines from the network, leave them on, preserve evidence, and call your insurer first. What's special is the pressure to pay. Don't make that decision alone or in a hurry — paying doesn't guarantee you get your data back, and it can carry legal and sanctions risk.

Your insurer and law enforcement help you weigh it, and free resources like CISA's StopRansomware.gov offer guidance and sometimes recovery tools. If you're a township or other public body, remember there's a special Ohio rule requiring a board vote before any ransom payment — our public-body guide covers it. Our ransomware guide walks the whole before-during-after.

! Don't let the countdown clock rush you

Ransom notes often show a ticking timer to panic you into paying fast. That pressure is the attacker's tool, not a real deadline you must obey. Isolate, preserve, and call your insurer — let the experts advise before any money moves.

Make sure your team knows the plan too

A hack might be first spotted by an employee, not you. The plan only works if the person who notices knows what to do.

Walk your staff through the basics: if your computer does something alarming — a ransom screen, files you can't open, accounts locked — **don't try to fix it, don't turn it off, and tell the owner right away**. The faster you hear about it, the faster the right response starts, and the less chance someone 'helpfully' wipes the evidence.

Make it clear there's no blame for reporting — even if they think they clicked something they shouldn't have. People hide mistakes out of fear, and that silence lets a small problem grow. A team that feels safe speaking up fast is one of your best defenses.

★ I'll brief your team in plain English

A short, friendly session so everyone knows the few first-hour rules — isolate, don't wipe, tell the boss — can save your business a world of trouble. I'm happy to come run it. Call (330) 200-8042.

Why this guide keeps mentioning insurance

You've noticed cyber insurance runs through this whole guide. Here's why it's so central to a good first hour.

A cyber policy isn't just money — it's a **response team on call**. When you phone that hotline, you instantly get forensics experts, breach lawyers, and recovery specialists coordinating on your behalf. For a small business, that's access to expertise you'd struggle to assemble yourself in a crisis, and it's exactly what turns a chaotic first hour into a managed one.

If you don't have a policy, this guide still works — you'll lean on trusted IT help and free government resources. But it's a strong argument for getting a quote once you're calm. Our cyber-insurance guides cover what a policy pays for and how to fill out the application honestly.

! 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.

Your first-hour plan, on one page

Here's the whole thing distilled to something you could follow with shaking hands. Print it and post it.

- ❑ **1. Breathe.** Don't rush. Your job is to not make it worse.
- ❑ **2. Isolate** affected machines from the network — leave them ON.
- ❑ **3. Preserve.** Delete nothing. Photograph the screen. Start a dated log.
- ❑ **4. Call your insurer's hotline FIRST** — policy number in hand.
- ❑ **5. Then IT help, then the FBI** at ic3.gov.
- ❑ **6. Change key passwords from a CLEAN device** — email first, turn on MFA.
- ❑ **7. Don't clean up** or rebuild until the experts say it's safe.

Seven lines. Tape them inside a drawer or by the main computer, make sure your team knows they're there, and you've turned the scariest hour in business into a checklist you can actually work through.

Common Questions

The questions owners ask me most about the first hour after a hack, answered plainly.

Q: Shouldn't I just turn the computer off to stop the attack?

No — disconnect it from the network instead, but leave it on. A running machine holds evidence in its memory that forensics may need, and powering off can erase it. Isolate, don't shut down, until the experts say otherwise.

Q: Why call the insurer before my IT person?

Because the insurer directs the whole response — they bring in forensics and legal experts, often at no extra cost, and many policies require you to notify them before spending on outside help. Calling them first protects both your recovery and your claim.

Q: Can I change my passwords right away?

Yes, but from a clean device the attacker hasn't touched — your phone or a different computer — not the compromised machine, which could capture the new ones. Start with email and turn on MFA. Coordinate with your insurer's team on timing.

Q: What if it turns out to be a false alarm?

Then you've lost nothing but a little time, and you've practiced the plan. It is always better to treat a possible breach seriously and be wrong than to dismiss a real one. No regrets for being careful.

Q: I don't have cyber insurance. What do I do first?

Isolate and preserve exactly the same way, then call a trusted IT professional as your first call, report to the FBI at ic3.gov, and use CISA's free resources. Afterward, strongly consider getting a policy for next time.

★ Think you've been hit right now?

Call me and I'll help you take the right first steps — what to unplug, what to leave alone, who to call in what order. Don't start deleting or rebooting — just call. (330) 200-8042.

You don't have to do this alone

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

I hope this guide made the first hour after a hack 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.

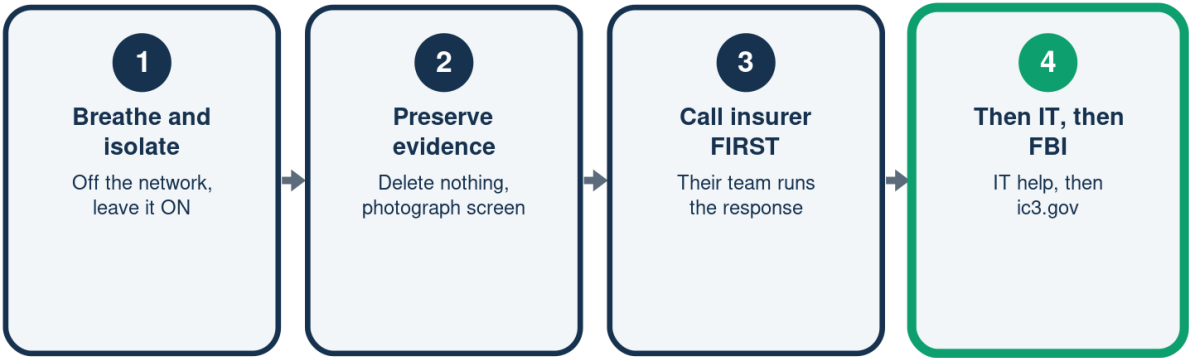
When you'd rather have a hand, that's exactly what I do. I come to your business, work at your pace, and never make you feel rushed or silly for asking. A first visit is a flat \$99, and for the parts that don't need me on-site I can often help right on your screen for \$49. Every visit comes with a 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 First Hour, In Order

Calm, correct moves beat fast ones



Change passwords from a clean device -- and don't clean up yet.

Do This, Not That

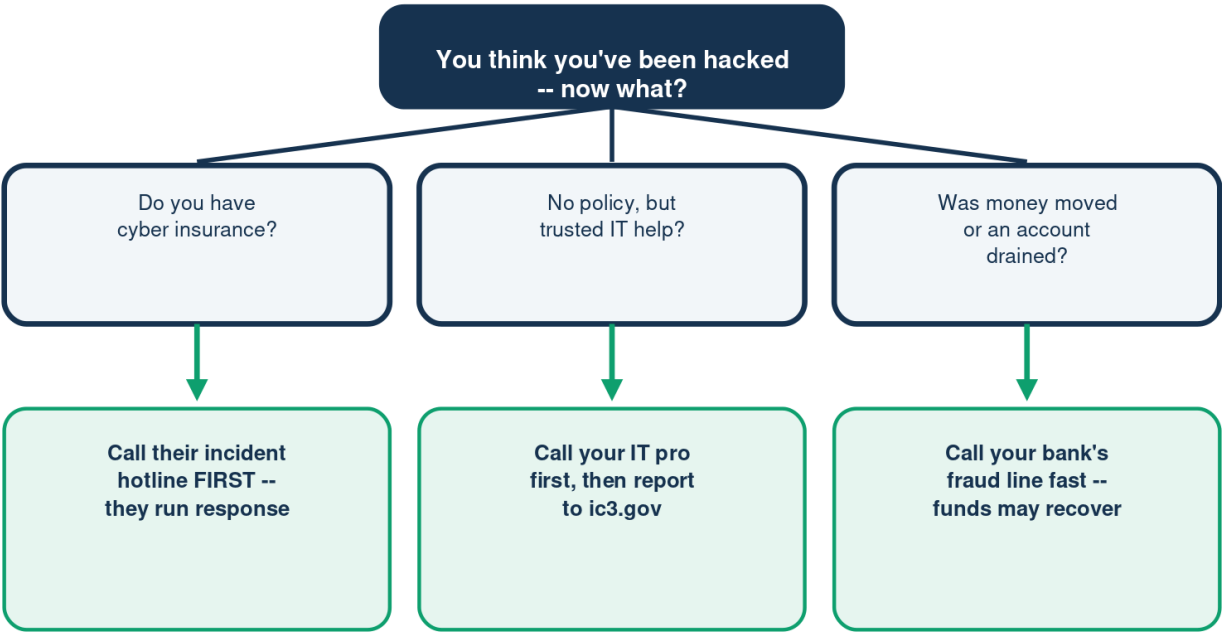
The moves people get backwards

	Do	Don't
The machine	Isolate it	Power off/wipe
The evidence	Preserve, photo	Delete files
First call	Insurer hotline	Fix it yourself
Passwords	Clean device	Infected PC

When in doubt, do nothing and make the call.

Who Do You Call, and When?

Order matters in the first hour



Preserve the scene before any call -- don't power off or delete.

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

Your Emergency Card

Numbers to have before you need them

	Have ready	Why
Insurer hotline	Policy number	Call first
IT helper	Bill's number	Hands-on help
Bank fraud line	If money moved	Fast recovery
FBI IC3	ic3.gov	Report crime

Keep it on paper -- it works even when every screen is locked.



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