



An Extended Guide · No. 2089

Free Help from CISA, NIST & CyberOhio: Scans, Checklists & Training

Government resources that cost
nothing — and how to sign up

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. Here's a happy surprise most owners miss: some of the best help for doing exactly that comes from the government, and it costs you nothing.

Good help that doesn't cost a dime

You already pay for a lot of things as a small-business owner. Cybersecurity help doesn't have to be one of them. Federal and Ohio programs offer free scans, plain-English checklists, and training — and most owners have never heard of them. This guide shows you what's out there and how to sign up.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. In 30+ years of helping folks and small businesses, I've learned that people skip free resources not because they don't want them, but because nobody ever pointed them out in plain language. So that's what I'll do here — no jargon, no sales pitch, just what exists and how to use it.

One honest caveat up front: government programs come and go, and their names, web addresses, and sign-up steps change. So I'll describe what each one does, and I'll always tell you to confirm it's still offered — and how to request it — on the official site. Think of this as a map, not a guarantee.

★ I'll help you actually use these

Knowing a free scan exists and getting it running are two different things. If you'd like a hand signing up for any of these or acting on what they tell you, that's exactly what I do. Call or text me at (330) 200-8042.

The whole guide, on one page

If you remember only these, you'll know where the free help lives and roughly what each offers.

- ❑ **CISA** (cisa.gov) offers free vulnerability scanning of your internet-facing systems, plus free guides and awareness campaigns.
- ❑ **NIST** (nist.gov) has a Small Business Cybersecurity Corner with plain guides and quick-start checklists built around its Cybersecurity Framework.
- ❑ **FBI IC3** (ic3.gov) is where you report internet crime, scam wire-transfers, and business-email fraud.
- ❑ **CyberOhio**, from the Ohio Attorney General's office, offers small-business training and resources.
- ❑ **CyberSECURE**, an Ohio Department of Development program, offers free one-on-one consulting to small businesses.
- ❑ Programs change — always **confirm current availability and sign-up** on the official site before you count on one.

! Only ever sign up on the official sites

Because these are free and worth having, scammers set up lookalike pages to collect your details. Type the official web address yourself — cisa.gov, nist.gov, ic3.gov — and be wary of 'sign up here' links in emails. A real government program will never cold-call demanding payment or passwords.

Why bother with government help?

A fair question. Here's what makes these programs genuinely worth your time, even as a busy owner.

First, they're made for you. These aren't dense manuals written for giant corporations — the small-business materials are deliberately plain, short, and practical, because the agencies know most of the country's businesses are small. Second, they're neutral. Nobody's trying to sell you software; the advice is the advice, with no commission attached.

Third, some of them do real work for you. A free vulnerability scan, for instance, actually checks your internet-facing systems and sends you a report — that's a service you might otherwise pay for. And using a recognized framework like the NIST Cybersecurity Framework can even matter legally in Ohio, which our safe-harbor guide explains.

You don't have to use all of them. Even picking one — a checklist to follow, a scan to request — puts you ahead of most small businesses. Treat this guide as a menu, not a to-do list.

✓ Free and neutral is a rare combination

Most cybersecurity advice comes from someone selling something. These government resources don't, which makes them a trustworthy starting point when you're trying to figure out what actually matters.

CISA: free scans and plain guides

CISA — the federal Cybersecurity and Infrastructure Security Agency, at cisa.gov — is probably the most useful single stop for a small business.

The standout offering is their Cyber Hygiene Services, which include free vulnerability scanning of your internet-facing systems — the parts of your network and website that face the public internet. You sign up, and they scan regularly and send you reports (commonly weekly) flagging weaknesses so you can fix them before someone else finds them. For a small business, that's a genuinely valuable free service.

Beyond scanning, CISA publishes free, plain-English guides, runs the Secure Our World awareness campaign (simple steps like MFA and strong passwords, aimed at regular people and small businesses), and maintains StopRansomware.gov as a one-stop hub for ransomware guidance and reporting.

✓ How to request the free scan

You request the Cyber Hygiene vulnerability scanning through CISA — look for 'Cyber Hygiene Services' on cisa.gov, where they list the current request method (historically by emailing vulnerability@cisa.dhs.gov). Because the exact sign-up can change, confirm the current steps on cisa.gov/cyber-hygiene-services before you begin.

What the free CISA scan does — and doesn't do

It's a terrific service, but it helps to know what it covers so you set the right expectations.

The vulnerability scanning looks at your internet-facing systems — things reachable from the public internet, like your website, mail server, or any device you've exposed online — and checks them for known weaknesses. You get regular reports showing what it found, so you (or someone helping you) can patch or close those gaps. It runs quietly in the background once set up.

What it isn't: it's not a replacement for the basics inside your office. It won't turn on your MFA, test your backups, or stop a staffer clicking a bad link. Think of it as a watchman checking the outside walls while you still lock the doors and windows yourself. Use it alongside the everyday habits in our other guides, not instead of them.

★ A scan report is only useful if you act on it

The reports can look technical, and a list of 'vulnerabilities' can be alarming if you don't know which matter. I'm happy to read a report with you, explain it in plain English, and help fix what actually needs fixing. Call (330) 200-8042.

NIST: checklists and a framework built for small business

NIST — the National Institute of Standards and Technology, at nist.gov — is the agency that writes the trusted recipes for security. And they've made a plain version just for small businesses.

Look for the NIST Small Business Cybersecurity Corner. It gathers plain-language guides and checklists aimed squarely at organizations like yours — no giant IT department assumed. It's a calm place to start when you want a trustworthy list of what to do, rather than a sales pitch for a product.

NIST is also behind the Cybersecurity Framework — CSF for short — a widely recognized way of organizing security into a handful of plain functions. The current edition, CSF 2.0, was released on February 26, 2024, and it added a 'Govern' function to the earlier set, emphasizing that leadership and good decisions sit at the center of security. It comes with small-business quick-start guides to make it approachable.

✓ The framework is the one that matters legally in Ohio

The NIST Cybersecurity Framework is one of the recognized frameworks behind Ohio's cybersecurity safe harbor. If you ever want the legal benefit our safe-harbor guide describes, building your written program around NIST CSF is a natural path — confirm the details with an attorney.

The framework in plain English

Don't let the word 'framework' scare you. It's really just a tidy way of grouping the things every business should think about.

The NIST Cybersecurity Framework organizes security into a small set of plain-language functions. You don't need to memorize them — you just need to see that they map neatly onto common sense, and onto the other guides in this series:

- **Govern:** decide who's responsible and make security a real priority — the newest piece in CSF 2.0.
- **Identify:** know what you have and what matters — your data, devices, and accounts.
- **Protect:** the everyday defenses — MFA, updates, access limits, training.
- **Detect:** notice when something's wrong.
- **Respond:** know what to do when it happens — who to call, what steps to take.
- **Recover:** get back to normal, with backups you've tested.

✓ You're already doing more of this than you think

If you've turned on MFA, you're 'protecting.' If you keep a tested backup, you're ready to 'recover.' The framework just gives a name to good habits and helps you spot the gaps.

FBI IC3: where to report internet crime

If you're ever hit by online fraud, this is the front door for reporting it — and reporting matters more than people realize.

The FBI's Internet Crime Complaint Center — IC3, at ic3.gov — is where businesses and individuals report internet crime: scam emails, fraudulent wire transfers, business-email compromise (where a crook poses as a vendor or boss to redirect a payment), ransomware, and the like. Filing a report is free and can be done online.

Why bother reporting, especially if the money's already gone? Two reasons. First, fast reporting — particularly on a fraudulent wire or payment — can sometimes help authorities freeze or recover funds, so time matters. Second, your report feeds the national picture that helps catch these crooks and warn others. Our guide on payment-redirection fraud and the one on the first hour after a hack both point here.

! Report a fraudulent payment fast — hours count

If you've sent money to a scammer by wire or transfer, don't wait. Contact your bank immediately and file with IC3 (ic3.gov) as soon as you can — quick action occasionally allows funds to be stopped. The longer you wait, the slimmer the chance.

CyberOhio: help from the Ohio Attorney General's office

Ohio has its own small-business cybersecurity effort, and it's aimed right at businesses your size.

CyberOhio is an initiative of the Ohio Attorney General's office, launched back in 2016, offering small-business cybersecurity training and resources. It's a natural fit for an Ohio business because it's built with our state's small businesses in mind, and it connects to Ohio's broader cybersecurity efforts — including the data-protection safe harbor our companion guide explains.

As with every program here, what's offered and how you access it can change over time, so check the Ohio Attorney General's office for the current CyberOhio offerings. It's a good place for an Ohio owner to look for training and plain guidance that fits our state's rules.

✓ A natural fit for an Ohio business

Because CyberOhio comes from our own state, its materials line up with Ohio's laws and programs. If you want resources that speak to where you actually do business, start here — and confirm the current offerings on the Attorney General's site.

Where to start depends on the time you have

All of these resources are free, but the right first pick depends on whether you want something quick to read or someone to talk to.

If you want to do it yourself, fast

You'd rather grab a checklist, request a scan, and work through it on your own schedule. The federal resources are perfect for this — they're self-serve and available any time.

- Start with the NIST Small Business Cybersecurity Corner for a plain checklist to follow.
- Request CISA's free vulnerability scan so something's actively watching your internet-facing systems.
- Bookmark ic3.gov now, so you know exactly where to report if fraud ever hits.
- Use CISA's Secure Our World pages to walk your staff through the basics.

If you'd rather have someone guide you

You'd get more from talking it through than from reading a PDF alone. Ohio's programs lean this way, offering training and even one-on-one help built for small businesses.

- Look into CyberSECURE, the Ohio Department of Development program offering free one-on-one consulting.
- Check CyberOhio, from the Ohio Attorney General's office, for small-business training.
- Pair any of it with a local hand — I can help you act on what the programs recommend.
- Confirm current availability and sign-up on the official state sites before you count on a program.

★ Not sure which free resource fits you?

Tell me whether you'd rather read-and-do or talk-it-through, and I'll point you to the right starting place — then help you actually use it. Call (330) 200-8042.

CyberSECURE: free one-on-one consulting for Ohio businesses

This one's a standout: actual people helping you, at no charge, through an Ohio program.

CyberSECURE is a program from the Ohio Department of Development, run together with the Ohio APEX Accelerators and the Ohio Small Business Development Centers (SBDC). The idea is free one-on-one consulting for small businesses — a knowledgeable person who can look at your situation and walk you through improving your cybersecurity, without charging you and without selling you anything.

For an owner who feels lost about where to begin, that kind of personal, no-cost guidance is hard to beat. As always, confirm the current availability and how to enroll through the Ohio Department of Development, the APEX Accelerators, or your local SBDC, since program details shift over time.

★ Free consulting and a local hand work well together

Programs like CyberSECURE are wonderful for the plan; I'm the fellow who can sit with you and actually turn the plan into settings that work. Use both — they complement each other. Call (330) 200-8042.

The resources at a glance

Here's the whole menu in one place, so you can see what each is for and who it suits.

Resource	What you get
CISA (cisa.gov)	Free vulnerability scanning, plain guides, ransomware help
NIST (nist.gov)	Small Business Corner checklists and the CSF framework
FBI IC3 (ic3.gov)	Where to report scams, fraud, and ransomware
CyberOhio	Ohio Attorney General's small-business training and resources
CyberSECURE	Ohio Dept. of Development free one-on-one consulting

None of these costs a thing. Pick the one that matches how you like to work — a scan, a checklist, a conversation — and start there. You can always add the others later.

! Confirm each one is still offered before you rely on it

This map is accurate as I write it, but government programs are renamed, moved, and sometimes retired. Always verify current availability and the sign-up steps on the official site before counting on a particular program.

Make sure you're on the real site

Because these programs are free and trusted, scammers imitate them. A minute of care keeps you safe.

Crooks build lookalike pages that mimic government sites, hoping to collect your details or trick you into 'paying a fee' for something that's actually free. The defense is simple: type the official address yourself rather than clicking a link in an email — cisa.gov, nist.gov, ic3.gov — and look for the real .gov address in your browser's bar.

- Real federal sites end in **.gov** — type it yourself rather than trusting a link.
- These programs are **free**; anyone demanding payment for 'CISA scanning' is a red flag.
- The government won't **cold-call** you demanding passwords or remote access.
- If an email pushes urgency to 'sign up now,' slow down and go to the site directly.

✓ When in doubt, navigate there yourself

The single best habit for any 'official' message is to ignore its links and go to the agency's real website on your own. If the offer is real, you'll find it there; if you can't, that tells you something too.

How these fit with the rest of your plan

Free resources are a wonderful boost, but they work best woven into the simple plan the rest of this series builds.

Think of these programs as tools, not the whole toolbox. CISA's scan watches your outside walls; NIST's checklist tells you which basics to cover; IC3 is your reporting line if the worst happens; Ohio's programs coach you through it. But the day-to-day work — turning on MFA, testing backups, training staff — is still yours to do, with whatever help you choose.

Our one-page security plan guide is a good anchor: use it to decide your handful of priorities, then pull in these free resources to help you hit them. For public bodies — a township, a village, a school office — our guide on political-subdivision rules points to these same programs plus the specific Ohio reporting duties that apply to you.

✓ Let the framework organize your plan

If you want one simple structure, use the NIST functions — govern, identify, protect, detect, respond, recover — as the headings of your one-page plan. Each free resource then slots neatly under one of them.

A special note for public and government offices

If you run a township, village, library, or other public body, these free resources matter even more — and so do some specific rules.

Public bodies are frequent targets and often run on tight budgets, so free federal and state help is especially welcome. CISA in particular works closely with state and local governments, and the NIST framework is a common foundation for a public body's required cybersecurity program.

Ohio also places specific duties on political subdivisions — adopting a cybersecurity program and reporting incidents to state offices within set timeframes. Those are beyond this guide's scope, but our guide for public bodies covers them, and it leans on exactly these free resources to help you meet them. If that's you, read the two guides together.

✓ Free help pairs well with the public-body rules

The same CISA scans and NIST checklists that help any small business also help a public body build the program Ohio now expects. Start free, then confirm the specific reporting duties with the Auditor of State's current guidance.

A gentle way to begin

Faced with a menu of programs, the trick is to pick just one and take a single step this week.

- ❑ Visit nist.gov and find the Small Business Cybersecurity Corner — skim one checklist.
- ❑ Go to cisa.gov/cyber-hygiene-services and read how to request the free scan.
- ❑ Bookmark ic3.gov now, so future-you knows exactly where to report fraud.
- ❑ Look up CyberOhio and CyberSECURE on the state sites to see what's currently offered.
- ❑ Pick one program and take one action — request the scan, or read one guide.

That's it. You don't have to engage with all five. One free scan running, or one checklist followed, makes you meaningfully safer than you were last week — and you can always come back for more.

★ I'll help you take the first step

If even starting feels like one more thing on a long list, let me handle the fiddly parts — finding the right page, requesting the scan, making sense of the first report. Call (330) 200-8042 and we'll knock it out.

Why I keep saying 'confirm it's still offered'

It's not me hedging — it's the honest truth about government programs, and it protects you.

Agencies rename things, move pages, launch new programs, and quietly retire old ones. A program that exists exactly as described today might have a new name or a new sign-up process a year from now. That's normal, and it's why every page here tells you to check the official site rather than trust a printed detail.

The good news is that the underlying ideas — free scans, plain checklists, a reporting line, training — tend to stick around even when the specifics shift. So if a program name doesn't match what you read here, don't give up; look on the agency's current site for the equivalent, or ask me to help you find where it moved.

✓ Trust the agency, verify the detail

Treat the agencies — CISA, NIST, the FBI, Ohio's offices — as the reliable part, and the exact program names and links as the part to double-check. That way you're never thrown by a change.

Using the free training with your staff

Some of the best free material is training you can put straight in front of your team — no expensive course required.

CISA's Secure Our World campaign and NIST's small-business materials include simple, friendly explanations of the core habits: strong passwords, turning on MFA, spotting phishing emails, and updating software. You can use these to walk your staff through the basics in a short meeting, without buying a training program or sounding like a lecture.

Keep it light and regular. A ten-minute chat built around one free handout — 'here's what a scam email looks like, here's what to do' — does more good than a once-a-year marathon nobody remembers. The free resources give you the content; you just provide the coffee and the time.

✓ Short and repeated beats long and rare

People retain a little, often, far better than a lot, once. Pick one topic from a free guide each month and spend a few minutes on it at a meeting you're already having.

Common Questions

The questions I hear most from owners about free government help, answered plainly.

Q: Is the CISA scan really free, with no catch?

Yes — CISA's Cyber Hygiene vulnerability scanning is a free government service. There's no fee and nothing to buy. Just make sure you request it through the real cisa.gov, since the exact sign-up can change and scammers imitate these offers.

Q: I'm not in a 'critical' industry — are these still for me?

Absolutely. The small-business materials from CISA and NIST, and Ohio's programs, are meant for ordinary small businesses — the plumber, the shop, the office. You don't have to be special or large to use them.

Q: Do I have to use the NIST framework to benefit?

No. You can grab a single checklist and stop there. But if you ever want Ohio's legal safe harbor, building your written program around a recognized framework like NIST CSF is the path — our safe-harbor guide explains it, and an attorney confirms the details.

Q: The program name in this guide doesn't match what I found online. Now what?

That's expected — names and pages change. Look on the agency's current official site for the equivalent offering, or give me a call and I'll help you find where it moved. Don't assume the help is gone just because a label changed.

★ Want a hand signing up for any of these?

I'm glad to help you request a scan, find the right checklist, or connect with an Ohio program — and then act on what they tell you. Call or text me and we'll get you set up. (330) 200-8042.

A quick, honest note

I want to be clear about what this guide is and isn't, so you use it with confidence.

This is a plain-English map of free resources, written by a local tech helper — it's general information, not legal advice, and not an official statement from any agency. I've described each program as accurately as I can from public information, but the agencies themselves are the final word on what they currently offer and how to access it.

So use this to know what's out there and what questions to ask, then confirm the specifics on the official sites. And for anything touching the law — like whether a framework helps you with Ohio's safe harbor — check with a qualified professional. That combination keeps you both informed and accurate.

! A quick, important note

This guide is a plain-English map of free resources, not legal advice and not an official statement from any agency. Program names, availability, and sign-up steps change, and any legal benefit of using a framework depends on your situation — so confirm current details on the official sites and check legal questions with a qualified professional.

The one thing to take away

If this guide leaves you with a single idea, let it be this.

There is real, trustworthy, no-cost help out there for a small business trying to get safer — and most owners never use it, simply because no one pointed the way. Now you know the names: CISA for scans and guides, NIST for checklists and the framework, IC3 to report fraud, and Ohio's CyberOhio and CyberSECURE for training and one-on-one help.

You don't have to do everything. Pick one, confirm it's still offered, and take a single step. Free help only helps if you reach for it — and you've just learned where to reach.

✓ Reaching for it is the whole trick

The owners who benefit aren't the ones who read about these programs — they're the ones who actually request the scan or follow the checklist. Be that owner. One small action this week is all it takes to start.

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 free cybersecurity help that's out there 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

Free Help at a Glance

What you get and who it's for

	What you get	Who it's for
CISA	Free scans, guides	Any small biz
NIST	Checklists, framework	DIY owners
FBI IC3	Report fraud	Anyone hit
CyberOhio	Training, resources	Ohio businesses
CyberSECURE	1-on-1 consulting	Ohio small biz

All free -- confirm current availability on the official sites.

Getting Started in Four Steps

Pick one program and begin



One step this week beats a long list you never start.

The NIST Framework, Plainly

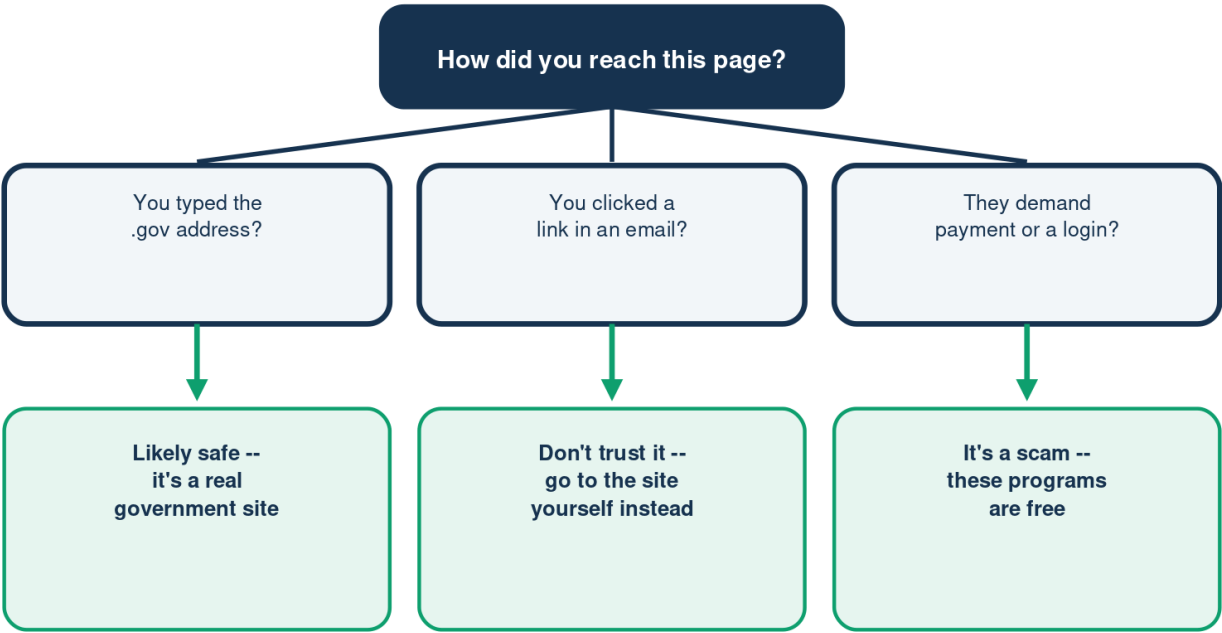
Common sense with tidy names

	Function	In plain English
Govern	The newest piece	Who's responsible
Identify / Protect	Know and defend	Data, MFA, updates
Detect / Respond	When it happens	Notice, then act
Recover	Bounce back	Tested backups

Govern is the newest piece, added in CSF 2.0.

Is This 'Official' Offer Real?

Avoid lookalike and scam sites



Government programs are free and never cold-call for passwords.

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



Need a Real Person?

You do not have to remember all of it.
You just have to remember you can call.
Friendly, in-person tech help -- I come to you.

BILL'S PROMISE

If you are not 100% happy with a visit, I will
make it right -- or refund it. No awkwardness,
no fine print. That is how I would want to be treated.

(330) 200-8042 · BillsHomeTech.com

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

— Bill

Prefer help without a visit?

Bill can screen-share and fix many things remotely — a flat \$49, free for Support Plan members.



A Note From Bill

A quick note from Bill.

I write these guides to make home tech a little less frustrating, and I do my best to keep every step accurate and up to date. Still, every home, device, and setup is a bit different, so I can't promise a guide will match yours exactly or fix your particular problem. These guides are for general information only — they're not professional, legal, or financial advice, and they don't replace your device's own manual or the manufacturer's instructions. Please go slow, use your own good judgment, and use everything here at your own risk. If a step involves electrical wiring, a gas appliance, a water heater, plumbing, or climbing a ladder — or if anything just doesn't feel safe — please stop and call a licensed professional (or give me a call at 330-200-8042). Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that comes from using these guides. Thanks for reading, and stay safe out there.

— *Bill*



Book a visit —
billshometech.com/book

Use of these guides is subject to our Terms of Use (billshometech.com/terms-of-use).

(330) 200-8042 · BillsHomeTech.com

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

For general information only — not professional advice. Use at your own risk. For electrical, gas, water, or ladder work, please call a licensed professional. — Bill's Home Tech