



An Extended Guide · No. 2070

A One-Page Security Plan for a Small Office

Who's in charge, what you protect,
the basics, and who to call

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. A one-page plan is simply those habits written down, plus the names and numbers you'd need on a bad day — so the knowledge lives on paper, not just in your head.

A security plan that really does fit on one page

You don't need a thick binder or a consultant to have a real security plan. For a small office, one honest page — who's in charge, what you're protecting, the basics you keep up, and who to call if something goes wrong — does the job. This guide helps you write it.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. I've spent 30+ years helping small businesses get their technology sorted out, in plain language and at a kitchen-table pace. I've watched too many owners put this off because they pictured something huge. It isn't huge. It's one page.

The value isn't in the paperwork — it's in the thinking. Writing it down forces the useful questions: who handles this, what matters most, what would we actually do if we got hit. A plan nobody wrote is a plan that lives in one person's head and vanishes the day they're out sick.

★ I'll help you write yours in one sitting

Bring me your coffee and an hour, and we'll fill in your one-page plan together — names, numbers, the basics — so it's real and done. No jargon, no overkill. Call or text me at (330) 200-8042.

The whole plan, on one page

A one-page security plan really only needs to answer four questions. Here they are.

- ❑ **Who's in charge?** Name the one person responsible for security decisions — usually you — and a backup.
- ❑ **What are we protecting?** A short list of your important data and the systems that hold it.
- ❑ **What basics do we keep up?** MFA everywhere, tested backups, updates current, and individual logins.
- ❑ **Who do we call if something goes wrong?** Insurer, IT help, bank, and how to reach people if the computers are down.
- ❑ Keep it to a page, date it, and review it a couple of times a year.
- ❑ This page is also the starting seed for bigger required plans if your business needs one — see our law guides.

✓ Short and current beats long and forgotten

A one-page plan you actually keep up to date is worth far more than a fifty-page document you wrote once and never opened again. The goal is a living page, not a binder on a shelf.

Why one page is the right size

The best plan is the one you'll actually write, keep, and use. For a small office, that's one page.

Big security documents fail small businesses for a simple reason: they're too much work to start and too much work to keep current, so they either never get written or go stale the moment anything changes. A single page sidesteps both problems. It's quick to write and quick to update.

One page also forces you to keep only what matters. You can't bury the important stuff — who to call, where the backups are, who's in charge — under pages of boilerplate, because there's no room for boilerplate. Everything on the page earns its place.

✓ If it grows, that's fine — but start at one page

Some businesses, by law or by size, do need a fuller written plan. Even then, this one page is the right first step — it becomes the summary at the front and the outline for the rest. Start here no matter where you'll end up.

Part one: who's in charge

Every plan needs a name. Somebody has to own security, or it quietly becomes nobody's job.

Write down the one person responsible for security decisions. In a small office that's usually you, the owner — and that's fine. The point isn't to create a title; it's to make sure there's a clear answer to 'who decides?' when a question or a problem comes up.

Then name a **backup** — a second person who knows where things are and can act if the first person is out sick, on vacation, or unreachable during an incident. If you're truly a one-person shop, your backup might be your spouse, your accountant, or the IT helper you trust. Just make sure someone else knows how to reach the key accounts.

! Don't let it all live in one head

The most common gap I see isn't a missing firewall — it's that one person holds every password and plan in their memory. If that person is unavailable on the worst day, the business is stuck. Writing it down, and naming a backup, fixes that quietly.

Part two: what you're protecting

You can't protect what you haven't named. A short inventory is the heart of the plan.

List your important data and the systems that hold it — not every file, just the things that would hurt to lose or to have leaked. For most small offices that's a short list: customer records, financial and accounting data, email, and whatever's unique to your trade.

Next to each, note where it lives: which cloud account, which computer, which service. The exercise usually surprises owners — you find data in places you'd forgotten, and old accounts nobody uses anymore. Both are worth knowing about.

- **Customer or member data** — names, contact info, anything sensitive like card or ID numbers.
- **Financial records** — accounting files, bank access, payroll.
- **Email and files** — where your day-to-day work lives.
- **Trade-specific systems** — scheduling, point-of-sale, design files, whatever runs your work.
- **The accounts that control all of it** — your domain, your Microsoft 365 or Google Workspace admin.

Part three: the basics you keep up

This is the short list of habits that stop most trouble. The plan just names them and says they're on.

You don't need a long controls list for a one-page plan. You need the handful that do the most work, written as plain statements you can point to and say 'yes, we do that.' These four carry most of the weight:

- ❑ **MFA everywhere** — a second sign-in step on email, cloud, admin, and remote access. See our Microsoft 365 and Google Workspace guides.
- ❑ **Tested backups** — your important data backed up where ransomware can't reach, and actually restored at least once.
- ❑ **Updates current** — security updates installed, and no software running past its end-of-support date.
- ❑ **Individual logins, least access** — everyone has their own account with only the access they need; no shared logins.

✓ Write what's true, then fix what isn't

Fill in each basic honestly today — 'MFA on email, not yet on remote access.' The gaps you write down become your short to-do list. A plan that names an honest gap is more useful than one that pretends everything's perfect.

Part four: who to call when something goes wrong

The worst time to go hunting for a phone number is during an actual emergency. Write them down now.

The last part of the page is a short call list for a bad day. When something goes wrong, you want to reach for the plan, not scramble. List who to call, in what order, and — importantly — how to reach them if the computers themselves are down.

- **Your insurer's incident hotline** and policy number — most cyber policies want you to call them first.
- **Your IT help** — me, or whoever keeps your systems running.
- **Your bank's fraud line** — if money or accounts are involved.
- **Key accounts** — where your domain and your main admin account live, so you can lock them down fast.
- **The FBI's IC3 (ic3.gov)** for internet crime and wire fraud.

! Keep a copy off the computers

If ransomware locks your systems, a plan saved only on those systems is useless. Keep a printed copy somewhere safe — a drawer, a binder at home — and maybe a photo on your phone, so the call list is reachable even when everything else is down.

The one-page template, laid out

Here's the whole page in order, so you can copy it onto a sheet and fill in the blanks.

Section	What to write
Who's in charge	Responsible person + backup person, with phone numbers.
What we protect	Short list of important data and where each lives.
The basics	MFA, backups, updates, individual logins — on or a dated to-do.
Who to call	Insurer, IT, bank, key accounts, IC3 — with numbers.
Dates	Date written and date of last review.

★ **Want a ready-to-fill version?**

I can hand you a clean one-page template and sit with you while we fill it in for your actual business — real names, real numbers, honest basics. One sitting and it's done. Call (330) 200-8042.

Fill it in honestly — gaps and all

A plan's job is to tell you the truth about where you stand, not to make you feel finished.

As you write each basic, resist the urge to tidy reality. If MFA is on for email but not for your remote-access tool, write exactly that. If you've got backups running but have never tested a restore, say so. The honest version is the useful version, because it shows you precisely what to fix.

Turn each honest gap into a dated line: 'Turn on MFA for remote access — by end of month.' Now your plan isn't just a snapshot; it's a short, realistic to-do list. Check the lines off as you close them, and your plan improves itself.

✓ An honest gap is worth more than a hopeful 'done'

Pretending a control is in place when it isn't helps no one — and if you ever carry cyber insurance, it can actually hurt you, since the application is a sworn statement. Our cyber-insurance application guide explains why honesty there is so important.

The same one page, a slightly different fill-in

Every small office needs the same four parts, but how much you write under each depends on whether it's just you or a team sharing the systems.

If you're a solo operator or a very small office

With one or a few people, the plan is wonderfully short. You're usually the person in charge and the only one with logins, so most of the page is a quick, honest snapshot you can finish in minutes.

- Name yourself as responsible, and pick one trusted backup who could reach your key accounts.
- Your 'what we protect' list is short — email, a cloud account, a laptop or two.
- The basics come down to your own good habits: MFA on, one tested backup, updates current.
- Keep the call list simple — insurer, me, your bank — on a card you can grab.

If you have employees sharing systems

More people means the plan has to cover how access is handled — who gets what, and what happens when someone joins or leaves. That's where a written page earns its keep, because the rules can't live in one person's memory.

- Spell out that everyone has their own login with only the access they need — no shared accounts.
- Add a line for cutting off access the day someone leaves — see our offboarding guide.
- Note who approves new accounts and admin rights, so it isn't ad-hoc.
- Include a basic rule for personal phones and home PCs used for work — see our BYOD guide.

★ Not sure how much to write for your size?

Tell me how many people touch your systems and I'll help you fill the page to fit — short and honest for a solo shop, a bit fuller for a team. Call (330) 200-8042.

Keeping the page alive

A plan is only as good as its last update. The good news: updating one page takes minutes.

Set a simple rhythm. Review the page a couple of times a year, and any time something changes — a new employee, a new cloud service, a new piece of equipment, a person who leaves. Each of those is a reason to glance at the page and bring it current.

Date every version. Writing 'last reviewed' at the bottom does two things: it tells you at a glance whether the plan is stale, and — if you ever need to show you take security seriously, for insurance or a client — it proves the plan is a living document, not a dusty one.

✓ Tie the review to something you already do

Pin the review to a date you won't forget — when you renew your insurance, do your taxes, or close the books for the year. Riding along with a habit you already have means the plan actually gets looked at.

When one page needs to grow

For some businesses, a written security plan isn't just smart — it's required. Your one page is where that starts.

Certain kinds of businesses are legally expected to keep a fuller written information security plan. If you prepare taxes, the IRS expects a written data security plan — see our tax-preparer plan guide. If you count as a 'financial institution' under the FTC Safeguards Rule — which catches more small businesses than you'd think — a written program is required. And Ohio's data-protection Safe Harbor rewards having one.

Here's the reassuring part: those bigger documents are built from the exact same bones as your one page. Who's responsible, what data you hold, what safeguards you keep, what you'd do in an incident — that's the skeleton of all of them. Start with the one page and you're already partway there.

! A quick, important note

Whether your business is legally required to keep a written security plan — and exactly what it must contain — is a legal question that depends on your trade and situation. This guide is general information, not legal advice. Our FTC Safeguards and tax-preparer guides explain the ideas, but confirm what applies to you with an attorney or the agency itself.

How the page connects to everything else

Your one-page plan isn't a standalone chore — it's the hub that ties your other security habits together.

Think of the page as the table of contents for how you run a safe shop. Each line points to something you do, and many of those have their own guide in this series. The plan keeps them all in one place so nothing gets quietly dropped.

- The **basics** lines connect to our MFA, backup fire-drill, and updates guides.
- The **who to call** line connects to our first-hour-after-a-hack and cyber-insurance guides.
- The **access** lines connect to our offboarding and BYOD guides.
- The **what we protect** list connects to our breach-notification and data-handling guides.

✓ Don't duplicate — just point

Your one page shouldn't repeat the detail of those other guides. It just needs to name the habit and, if helpful, note where the fuller instructions live. Keep the page a summary; let the guides hold the how-to.

A note on passwords and key accounts

Two account details belong on — or close to — your page, because they decide who really controls your business online.

First, the keys to the kingdom: your domain registrar (where your web and email address live) and your primary admin account for Microsoft 365 or Google Workspace. Note who holds these and make sure it's you or someone you fully trust. Whoever controls these controls everything, so never hand over the only copy — see our hiring-IT-help guide.

Second, how your team handles passwords. You don't need to list passwords on the plan — please don't. Just note the rule: strong, unique passwords, not reused across sites, kept somewhere safe rather than on sticky notes. MFA is what backs all of this up when a password slips out.

! Never write actual passwords on the plan

The plan should say where passwords are kept and what the rules are — never the passwords themselves. A document listing live passwords is a gift to anyone who finds it. Keep the secrets in a proper password manager, not on the page you pass around.

The 'if we get hit' corner

A few short lines about what to do in an incident turn panic into a checklist. Give them a corner of the page.

You don't need an elaborate incident plan on one page — you need enough to keep a scared person from making things worse in the first confusing minutes. A short reminder does that: stay calm, isolate, call the right people in order, and don't start 'cleaning up' before you're told to.

- ❑ Stay calm — disconnect the affected machine from the network, but don't power it off if your insurer may want it preserved.
- ❑ Call the insurer's incident hotline first — they direct the response.
- ❑ Then call your IT help; then your bank if money's involved; then the FBI's IC3 at ic3.gov.
- ❑ Change important passwords from a clean device, not the hit one.
- ❑ Don't wipe, reinstall, or 'tidy up' before you're told to — you may destroy evidence.

✓ Our first-hour guide expands this corner

This is the two-inch version of a bigger idea. Our guide 'The First Hour After a Hack' walks through exactly why the order matters and why you isolate rather than power off. Pair the two.

Who should see the plan

A plan helps only the people who've actually seen it. Share it — carefully.

Everyone who touches your systems should know the plan exists, know who's in charge, and know what to do in the 'if we get hit' corner. They don't all need every detail, but the call list and the incident steps should be no mystery to anyone who might be the one at the desk when trouble starts.

At the same time, treat the plan as sensitive. It describes how your business is protected, so it shouldn't be left lying out for a visitor or posted publicly. Share it with your team, keep a copy with your business papers and a copy off-site, and don't hand it to people who don't need it.

✓ Walk the team through it once, out loud

A five-minute walk-through where everyone hears 'here's who's in charge, here's what to do if something looks wrong' does more than any email. People remember what they discussed; they forget what they were merely sent.

The mistakes that make a plan useless

A plan can exist and still fail you. These are the ways it happens — and now you'll avoid them.

- **Making it too big** — a long document you never update is worse than a current one page.
- **Writing hopeful fiction** — listing controls that aren't really on. Write the truth and a to-do.
- **Keeping it only on the computers** that could be locked in an incident. Keep a printed copy.
- **Listing live passwords** on the plan. Note where they're kept, never the secrets themselves.
- **Never reviewing it** — a plan that's two years stale describes a business you no longer run.
- **Letting it live in one head** — no backup person, no written copy.

! A forgotten plan gives false comfort

The danger of a stale or fictional plan is that it makes you feel protected when you aren't. Better an honest one page you trust than a thick document you're quietly unsure about. Keep it true and keep it current.

Write yours this week

This is genuinely an afternoon's task. Here's the short list to get it done.

- ❑ Grab one sheet and write the four headings: who's in charge, what we protect, the basics, who to call.
- ❑ Fill in the responsible person and a backup, with phone numbers.
- ❑ List your important data and where each piece lives.
- ❑ Mark each basic honestly — on, or a dated to-do.
- ❑ Write your call list with numbers, and note how to reach people if the computers are down.
- ❑ Date it, print a copy for off the computers, and put a review on your calendar.

★ Let's knock it out together

If a blank page is what's stopping you, that's exactly where I help most. One sitting, your real details, an honest plan you'll actually use — and we'll close the easy gaps while we're at it. Call (330) 200-8042.

A plan that proves you take security seriously

Beyond protecting you, a current written plan quietly helps in several ways you may not expect.

A dated, honest plan is evidence of good-faith effort. If you apply for cyber insurance, it helps you answer the application and shows an underwriter you run a careful shop. If a client or contract asks about your security, you have a clear answer. And in Ohio, maintaining a written cybersecurity program is the heart of the Safe Harbor our Ohio Safe Harbor guide explains.

None of that is the main reason to write the plan — the main reason is that it genuinely makes you safer. But it's a nice bonus that the same one page that protects you also helps you look — and be — credible when someone asks.

✓ Keep your dated versions

Don't throw away last year's plan when you update it. A little trail of dated versions shows the plan is a living habit, which is exactly what insurers, clients, and the Safe Harbor idea are looking for.

A simple system you can keep forever

Make the plan effortless to maintain by pairing it with two small living lists.

- ❑ The **one-page plan** itself — who's in charge, what you protect, the basics, who to call.
- ❑ An **accounts-and-MFA list** — every service you sign into and whether MFA is on.
- ❑ A **backup log** — what you back up and the date of your last tested restore.

Keep those three in one labeled folder — physical, digital, or both — and your whole security picture is visible at a glance. It's the same tidy habit behind our cyber-insurance application guide, and it makes renewals, audits, and bad days far calmer.

✓ Three living pages beat one dead binder

You're not building a compliance library. Three short pages you actually keep current tell you more about your real security than a thick manual gathering dust ever could.

Common Questions

The questions I hear most from owners sitting down to write a security plan, answered plainly.

Q: Can a security plan really fit on one page?

For most small offices, yes. One honest page — who's in charge, what you protect, the basics you keep up, and who to call — covers what matters. Some businesses need a fuller written plan by law, but even then the one page is the right starting point.

Q: Do I need special software or a template to write it?

No. A plain sheet of paper or a simple document works fine. The value is in the thinking, not the format. I'm happy to give you a clean template to fill in, but a handwritten page is a real plan too.

Q: What if I write down gaps — doesn't that look bad?

The opposite — it's exactly right. An honest gap turned into a dated to-do is the most useful thing on the page. Pretending everything's perfect helps no one and, if you carry cyber insurance, can actually hurt you.

Q: How often should I update it?

Review it a couple of times a year and whenever something changes — a new person, a new service, a departure. Updating one page takes minutes. Tie the review to something you already do, like insurance renewal, so it doesn't get forgotten.

Q: Is this the same as the plan the IRS or FTC requires?

It's the seed of it. Those required plans are built from the same bones — who's responsible, what data you hold, your safeguards, your incident steps — just with more detail. Start here; see our tax-preparer and FTC Safeguards guides if those apply to you.

★ Staring at a blank page?

That's the hardest part, and it's where I help most. Give me a call and we'll fill in your one-page plan together, in plain English, in a single sitting. 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 your one-page security plan 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 Four Parts of the Page

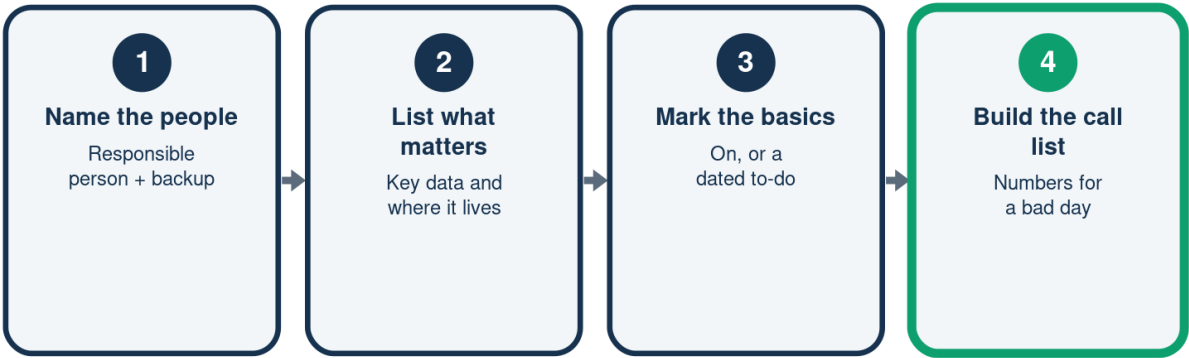
Everything a small-office plan needs

	What to write	Example
Who's in charge	Responsible person	Owner + a backup
What we protect	Key data + where	Clients, email
The basics	MFA, backups	Updates, logins
Who to call	Your call list	Insurer, IT, bank

One honest page, dated and reviewed, beats a binder you never open.

Write It in Four Steps

An afternoon's task, done calmly



Date it, print a copy off the computers, and set a review reminder.

A Living Page vs a Dead Binder

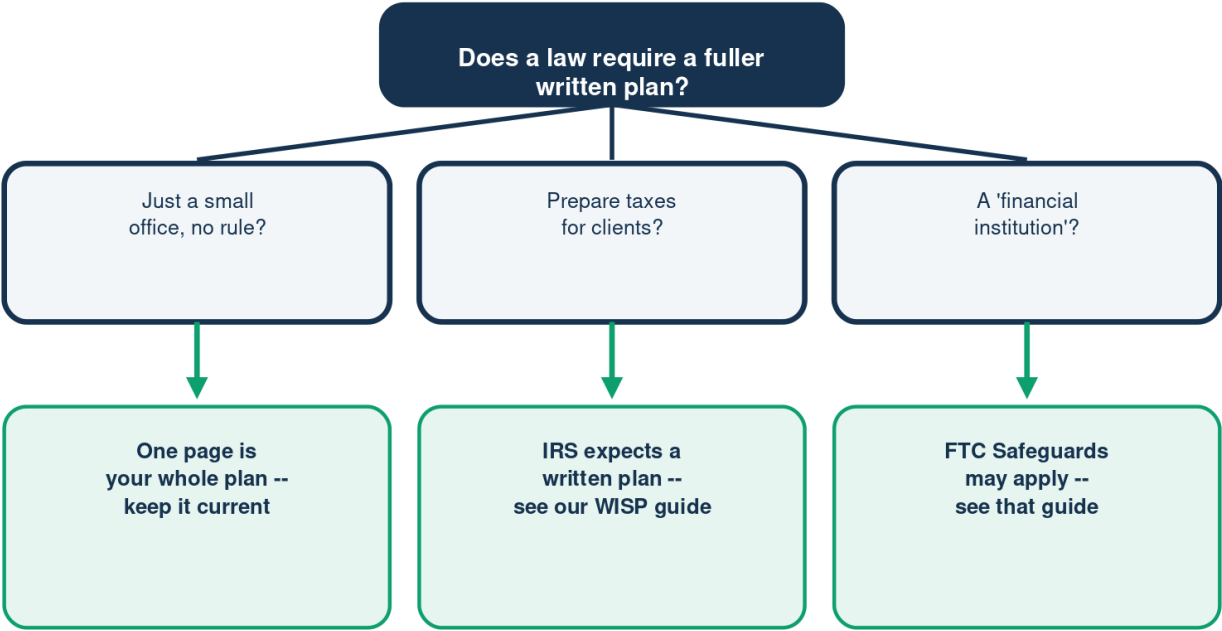
Why one honest page wins

	Living one page	Dead binder
Length	One sheet	Dozens of pages
Updated	A few times/yr	Written once
Honesty	Gaps + to-dos	Hopeful fiction
Used	Grabbed on bad day	On a shelf

Short and current beats long and forgotten, every time.

One Page, or Does It Grow?

Start at one page no matter the answer



Whether a law applies to you is a legal question -- confirm it.

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