



An Extended Guide · No. 2088

Churches & Nonprofits: Volunteers, Donor Lists & Shared Logins

Protect member and donor data when
most of your users are volunteers

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 congregation or a cause runs on trust, and part of honoring that trust is guarding the names, gifts, and personal details people share with you.

Protecting the people who trust your mission

Churches and nonprofits carry something precious: lists of members, donors, and the families you serve. You also run mostly on volunteers, who come and go. This guide shows how to keep that information safe without turning your welcoming ministry into a fortress.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. I've spent 30+ years helping folks and small organizations with their technology, always in plain language and never in a rush. I have real respect for the work faith and community groups do, and I know you'd rather spend on your mission than on computers. Good news: the most important steps here cost little or nothing.

The whole idea comes down to this: give each person their own login, let people see only what they need, turn on a second sign-in step, guard your giving platform and donor lists, and hand off cleanly when a volunteer moves on. We'll take each one gently.

★ I'm glad to help your organization

If any of this feels overwhelming, you're in good company — most offices haven't set this up, and there's no shame in that. I can come sit with your office team or a volunteer and get it sorted. Call or text me at (330) 200-8042.

The whole guide, on one page

If you remember only these things, you'll protect your people and your mission from the most common troubles.

- ❑ Give each volunteer and staffer their **own login** — never one shared account the whole office uses.
- ❑ Let people see **only what they need** for their role — the nursery scheduler doesn't need the donor list.
- ❑ Turn on **MFA** (a second sign-in step) for everyone, especially office staff and anyone who touches money.
- ❑ **Lock down the giving platform** — that's where donations and card details flow, so it deserves the strongest protection.
- ❑ Treat your **donor and member lists** like the sensitive data they are — limited access, backed up, not emailed around.
- ❑ When a volunteer **rotates off**, remove their access that same week, just as you would for paid staff.

! The shared office login is the usual weak spot

The most common setup I see in a church or nonprofit office is one password that everyone — staff and volunteers alike — uses for everything. It feels friendly and simple, but it means no one can tell who did what, and the password leaks the first time a volunteer leaves. Individual logins fix almost all of this.

Why your organization is worth protecting

It's tempting to think 'we're small, nobody would bother with us.' Here's why that isn't quite true — and why it's fixable.

Crooks don't target you because you're big. They target you because the information is valuable and the doors are often open. A donor list is a list of generous people with money to give — exactly who a scammer wants to impersonate you to. Member records hold names, addresses, sometimes children's details. That's worth guarding for its own sake.

Your volunteer model adds a wrinkle. Paid staff get trained and offboarded; volunteers often don't. People help for a season and drift away, and their access — to the email, the member database, the giving platform — tends to drift right along with them, still active. None of this means your volunteers aren't trustworthy. It means access should follow the role, not linger after the person has moved on.

The reassuring part: the fixes are the same simple habits every small organization needs, and they're mostly free. You don't need a big budget to do right by the people who trust you.

✓ Guarding the data is part of the mission

Protecting a donor's information is simply another way of honoring their gift, and protecting a member's details is part of caring for them. Framed that way, this work belongs right alongside everything else you do.

Give everyone their own login

This single change does more good than almost anything else, and it's usually free.

One shared office password feels convenient, but it quietly costs you everything that makes access safe. With a shared login, you can't tell who sent an email or changed a record, you can't remove one person without locking out everyone, and the password spreads by word of mouth until no one knows who still has it.

Individual logins fix all of that. Each person signs in as themselves, the records show who did what, and when someone leaves you simply turn off their account — no need to change a password the whole office has to relearn. Most email and membership systems let you create individual users at no extra cost; it's just a matter of setting them up.

★ Setting up individual logins is a great first visit

If your office runs on one shared password, untangling it into individual logins is often the first thing I help an organization do. It's straightforward, and I can do it with your team in a visit or two. Call (330) 200-8042.

Let people see only what they need

Kindness and openness are wonderful in a community. With data, a little restraint is its own kindness.

Not everyone who helps needs to see everything. The person who schedules the nursery doesn't need the donor giving history; the newsletter volunteer doesn't need members' financial details. Giving each person access only to what their role requires — sometimes called 'least privilege' — protects everyone, including the volunteers themselves.

This isn't about distrust. It's about limiting how much can go wrong from any one account. If a volunteer's login is ever stolen or misused, the damage is contained to what that role could touch. It also spares a well-meaning helper from accidentally seeing or changing sensitive records they never needed in the first place.

Role	What they usually need
Office / admin staff	Most systems, including member records
Finance / treasurer	Giving platform, donation records
Event / program volunteer	Just their event or program tools
Communications	Newsletter and website — not donor data

✓ **Start roles small, add as needed**

It's far easier to grant a bit more access when someone genuinely needs it than to claw back access you handed out too freely. Begin each role with the minimum and expand only on request.

Turn on a second sign-in step

If individual logins are the foundation, this is the lock on the door — and it stops the most common break-in cold.

MFA — multi-factor authentication, also called two-step or two-factor sign-in — means a password alone can't get someone in. There's a second step: a code from an app or a tap on a phone. Because most break-ins start with a stolen or guessed password, this one setting defeats the great majority of them.

Turn it on for everyone who signs in, and be especially sure it's on for office staff, anyone with access to member records, and anyone who touches money or the giving platform.

Volunteers may grumble at one extra tap; a gentle explanation — 'this protects our members' information' — usually wins them over. Our Microsoft 365 and Google Workspace guides show exactly how to switch it on.

! MFA is the highest-value free step you can take

Across every kind of organization, turning on a second sign-in step is the single most effective protection against account break-ins — and it costs nothing. If you do just one thing from this guide, make it this, starting with the office and finance accounts.

Lock down your donation and giving platform

This is where money and card details flow, so it earns your strongest care and your fewest hands.

Whether you take gifts online, by text, or through a kiosk in the lobby, your giving platform is both the heart of your fundraising and a tempting target. Keep the circle of people who can sign into its settings small — ideally just a trusted staffer or two and your treasurer — and make sure every one of them uses MFA.

- Limit who can log into the platform's **settings**, not just who can see totals.
- Require **MFA** on every account that can reach it.
- Watch for anyone changing the **bank account** where donations are deposited — verify such changes carefully.
- Remove platform access the moment a treasurer or volunteer **rotates off**.
- Keep the platform and any connected software **up to date**.

! Watch for 'change our deposit account' requests

A classic fraud is an email that looks like it's from a board member or staffer asking to redirect donations to a new bank account. Always confirm any change to where money goes by calling the person on a known number first — never act on the email alone.

Treat donor and member lists like the treasure they are

These lists are among your most valuable — and most sensitive — possessions. Handle them with that in mind.

A donor or member list isn't just names. It can hold addresses, giving histories, phone numbers, family details, sometimes children's information. In the wrong hands it's a gift to scammers and a breach of the trust people placed in you. So keep it in one well-protected place, let only the roles that truly need it see it, and don't let copies scatter.

The most common mistake is casual copies: a spreadsheet emailed to a volunteer, downloaded to a home laptop, left on a thumb drive. Each copy is another place the list could leak from. Keep the real list in your member or donor system, pull only what a task needs, and delete working copies when the task is done. And make sure the list is backed up, so a crashed computer or a ransomware scare never means losing it.

✓ One home for the list, few copies

Decide where the real list lives, protect that spot well, and treat every copy as a temporary loan that gets deleted after use. Fewer copies means fewer ways for it to slip out.

A gentle word about rules that may apply

Handling donor financial information can bring extra responsibilities. You don't need to be an expert — you need to know when to ask one.

Because nonprofits often collect donations, card numbers, and bank details, some of the same rules that cover businesses handling financial or personal information can touch your organization too. There are frameworks and state notification rules that may come into play if sensitive data is ever exposed. Our guides on the FTC Safeguards Rule and on Ohio's breach-notification law explain those ideas in plain English.

I'm raising this only so it's on your radar, not to alarm you. Whether any particular rule applies to your organization is a question for a professional who knows your situation. The smart move is simply to protect the data well — which this guide helps you do — and to ask a knowledgeable attorney or advisor if you're ever unsure what's required.

! A quick, important note

This guide explains these ideas in plain English so you know what to ask about — it is general information, not legal advice, and whether any specific rule applies to your organization depends on your situation. Rules change, so please confirm what you're responsible for with an attorney or a qualified advisor before you rely on it.

A small congregation and a larger nonprofit, same principles

The core ideas — individual logins, least privilege, MFA, a guarded giving platform — fit any size. What changes is how many hands are involved and how formal your handoffs need to be.

If you're a small church or all-volunteer group

With a handful of helpers and maybe one part-time office person, you can set this up quickly. Your biggest risks are the shared office password and the volunteer who moved away a year ago but whose login still works.

- Replace the one shared password with an individual login for each regular helper.
- Turn on MFA for the office email, the giving platform, and the member list first.
- Keep a short list of who has access to what, so nothing gets forgotten as helpers change.
- When a volunteer stops helping, turn off their access that week — a quick note on the calendar makes it a habit.

If you're a larger nonprofit with staff and many volunteers

More people and more data mean the questions about roles, offboarding, and donor protection apply squarely to you. A little structure keeps a big, warm organization from leaking access everywhere.

- Define roles so each volunteer sees only their program's tools, not the donor database.
- Require MFA across the board, and especially on finance and administrator accounts.
- Build a real offboarding routine for volunteers and staff alike — our offboarding guide walks through it.
- Keep donor lists in one protected system and limit who can export or email them.

★ Not sure where to start with your organization?

Tell me how your office runs — how many volunteers, what you use for email and giving — and I'll help you set up individual logins and sensible roles without disrupting your good work. Call (330) 200-8042.

A clean handoff when volunteers rotate off

Volunteers coming and going is the rhythm of your work. Make their departure as tidy as their welcome.

When a volunteer or staff member stops helping — whether they move away, change churches, or simply step back for a season — their access should end too. This isn't a comment on anyone's character; it's the same care you'd take with a building key. A login left active is a door nobody is watching, and in a volunteer-heavy organization those doors pile up fast.

Keep it simple: when someone rotates off, turn off their logins, remove them from the giving platform and member system, and make sure any organization files on their personal device are returned or deleted. Our offboarding guide covers this same routine in more depth — the principles are identical whether the person was paid or volunteered.

✓ Tie it to your volunteer records

If you track volunteers on a roster or sign-up, add one line: 'access removed, date.'

That turns offboarding from something you hope someone remembers into something your records guarantee.

The scams that target good-hearted organizations

Scammers know your people want to help. They use that generosity against you — so a little healthy caution protects everyone.

A common trick aimed at churches and nonprofits is the 'gift-card request': an email that looks like it's from your pastor, director, or a board member, urgently asking a staffer or volunteer to buy gift cards or send money for someone in need. The urgency and the trusted name are the whole scam. Real leaders rarely ask for gift cards by surprise email.

The defense is a simple rule everyone can follow: any surprise request to buy cards, move money, or change where donations go gets verified by voice first — call the person on a number you already have, not one in the email. Give your volunteers explicit permission to pause and check. Nobody should feel they'll get in trouble for confirming.

! Urgency plus a trusted name is the warning sign

'I'm in a meeting, can't talk, just need you to grab some gift cards right now' is a script, not a real request. The moment an email combines urgency, secrecy, and money, slow down and verify by phone.

Make sure your lists survive a bad day

Protecting data isn't only about keeping others out — it's also about not losing it yourself.

A crashed computer, a ransomware scare, or an accidental deletion can wipe out a member list or giving history in an instant. A backup is your safety net — a separate copy you can restore from. For most small organizations, the member and donor systems keep their own backups, but don't assume; confirm it, and back up anything important that lives only on an office computer.

And remember: a backup you've never tried to restore is just a hope. Once in a while, confirm you can actually get a file or a list back from it. That small test is the difference between a backup that works and one that only looked like it did.

★ I can check your backups with you

Many offices think they're backed up and aren't — or have never tested it. I can confirm what's actually protected and set up anything that's missing, in plain terms. Call (330) 200-8042.

Who holds the master keys?

Every system has a top-level account that can change everything. Know who holds yours — and don't let it ride on one volunteer.

Your email system, your member database, your website, your giving platform — each has an administrator or 'owner' account that can add users, change settings, and remove protections. These master keys deserve special care: protect them with MFA, keep the number of people who hold them small, and make sure a key never rests with a single volunteer who might move away without passing it on.

A common and painful situation is discovering that the only person who could get into the website or the email settings left the organization months ago. Make sure a trusted staff member or officer — not just a helpful volunteer — always holds the master keys. Our guide on admin accounts goes deeper on keeping these powerful logins safe and separate.

! Don't let the only key leave with a volunteer

Before any volunteer who set up a system steps back, confirm the organization still holds the master login. 'Only Dave had that password, and Dave moved to Florida' is a story I'd love to help you never tell.

Put it on one page the office can follow

A short written plan means the next volunteer or new staffer inherits good habits instead of guesswork.

You don't need a thick policy binder. A single page, kept with your important documents, is enough to carry these habits from one group of helpers to the next. Volunteers turn over; a written page doesn't. Here's what to capture:

- ❑ Everyone gets an individual login — no shared office password.
- ❑ Each role sees only what it needs; the donor list stays limited.
- ❑ MFA is on for all accounts, especially office, finance, and giving.
- ❑ Surprise money or gift-card requests are verified by phone first.
- ❑ When a volunteer or staffer rotates off, we remove access that week.
- ❑ We know who holds the master keys, and the organization always has a copy.

✓ Hand it to every new helper

Make this page part of welcoming a new volunteer. When good habits are written down and handed over, your protection survives every rotation of the people who serve.

Keeping it warm, not rigid

You can be careful with data and still be the welcoming, trusting community you are. The two go together.

Some worry that locking things down will make their organization feel cold or suspicious of its own people. It doesn't have to. Individual logins, sensible roles, and a second sign-in step are quiet background habits — your volunteers barely notice them after the first week, and they protect the very people you serve.

Explain the 'why' and most folks embrace it: 'we do this to protect our members' and donors' information' is a reason people believe in. Frame security as part of your care for the community, not as distrust of your helpers, and it becomes something your organization is proud of rather than something it resents.

✓ Lead with the reason, not the rule

People follow a rule they understand. A sentence of 'here's why this keeps our members safe' does more than a page of 'you must' ever will.

Tools change — confirm the current way

Giving platforms and member systems update their menus often. The goal stays the same even when the buttons move.

Where you turn on MFA, how you set roles, how you remove a departed volunteer — the exact steps differ from one system to the next and change over time as software updates. Don't be discouraged if a menu doesn't match what a friend described. Look for the plain goals: a second sign-in step, roles that limit access, a way to turn off a login.

When you can't find a setting, check your system's current help pages or ask someone you trust to find it with you. It's always better to confirm than to assume something's protected when it isn't.

★ Can't find the setting? Call me

Menus move, and every platform hides things somewhere different. I keep up with where these controls live and I'm happy to find them with your team, in a visit or right on your screen. (330) 200-8042.

Give it a look once a year

A short yearly review keeps access from piling up as helpers come and go.

Pick a date you'll remember — the start of your program year, your annual meeting, tax season — and spend a half hour reviewing who has access to what. Remove logins for anyone who's rotated off, confirm MFA is still on, check that the master keys are accounted for, and make sure your lists are still backed up. Then date it so you know it's current.

In a volunteer-driven organization, this one habit matters more than almost anywhere else, because your people change so often. A yearly sweep keeps the tidy setup from quietly drifting back into a tangle of forgotten logins.

✓ Fold it into an existing meeting

Attach this review to something you already do each year — a board meeting, an annual report. It takes less time than people fear, and it keeps your protection honest.

If you think information was exposed

Even careful organizations have scares. Knowing the calm first steps keeps a scare from becoming a crisis.

If you suspect a donor list leaked, an account was broken into, or money was redirected, don't panic and don't try to quietly clean it up alone. Change the passwords on affected accounts from a device you trust, make sure MFA is on, and preserve what you can rather than deleting things. Then get the right help — a knowledgeable advisor, and for financial fraud, the authorities.

Because donor financial information may be involved, there could be obligations about notifying people — which is exactly when to call a professional rather than guess. Our guides on breach notification and the first steps after an incident walk through this calmly. The main thing: slow, careful, and with the right help beats fast and alone.

! Don't stay quiet to avoid embarrassment

The instinct to handle a breach privately, so no one worries, is natural and understandable — and it's usually the wrong call. Getting help early protects your members and your organization far better than silence.

Common Questions

The questions I hear most from church offices and nonprofit teams, answered plainly.

Q: We're all volunteers and we trust each other — do we really need separate logins?

Yes, and it isn't about distrust. Separate logins mean you can tell who did what, you can remove one person when they move on without locking out everyone, and no password spreads by word of mouth. It's good stewardship, not suspicion.

Q: Isn't this going to cost money we'd rather spend on our mission?

The most important steps — individual logins, MFA, sensible roles, clean offboarding — are usually free or already included in what you pay for email and your member system. This is mostly about setup and habits, not new spending.

Q: A volunteer set up our website and then left. What do we do?

Confirm the organization still holds the master login before anything else. If only that volunteer could get in, that's the first thing to fix — reach out while they're still willing to help, and make sure a trusted staffer or officer holds a copy of every key.

Q: Someone emailed asking us to buy gift cards for a family in need — is that real?

Treat a surprise gift-card or money request as a scam until you've confirmed it by voice. Call the person it claims to be from on a number you already have. Real leaders rarely ask for gift cards by urgent email.

★ Still have a question? There's no silly one

Churches and nonprofits are some of my favorite folks to help, and no question is too basic. Call or text me and we'll work through it together, gently and in plain English. (330) 200-8042.

Where to begin this week

You don't have to do everything at once. Here's a gentle order that gets the biggest protection first.

- **This week:** turn on MFA for the office email, the giving platform, and anyone who touches money.
- **Next:** replace the shared office password with an individual login for each regular helper.
- **Then:** set roles so each person sees only what they need, especially around the donor list.
- **Soon:** write your one-page plan and start removing access when volunteers rotate off.
- **Ongoing:** confirm your backups work and review access once a year.

Each step stands on its own and makes you safer than you were yesterday. Progress, not perfection, is the goal — and every one of these is something a willing volunteer or a visit from me can knock out.

✓ One step at a time is plenty

Don't let the full list overwhelm you. Turn on MFA this week and you've already closed the most common door. Everything after that is a bonus you can add at your own pace.

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 protecting your members and donors 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

Shared Login vs Individual Logins

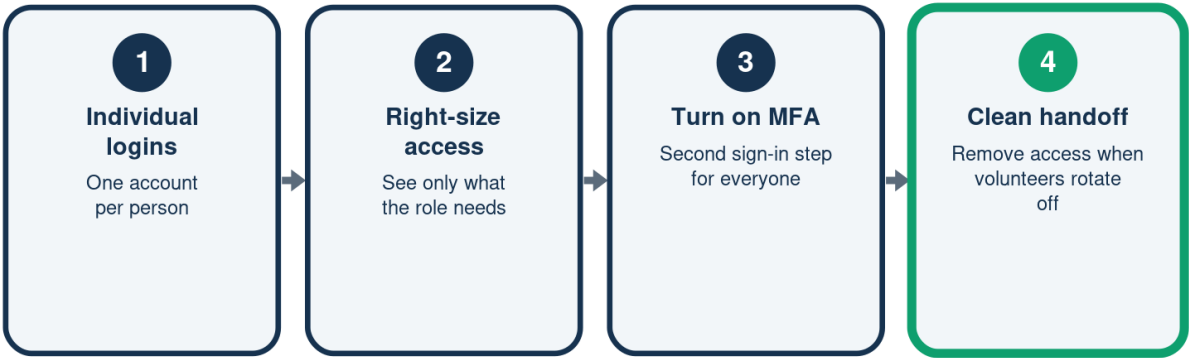
Why one login each protects your people

	Shared office login	Individual logins
Who did what	No way to tell	Records show who
A volunteer leaves	Reset for all	Turn off just one
The password	Spreads by mouth	Stays with one
Donor list access	Everyone can see	Only roles that need

Individual logins fix most church and nonprofit risks at once.

Setting Up Safely

Four gentle steps for your office



Guard the giving platform and donor list most of all.

Who Should See What

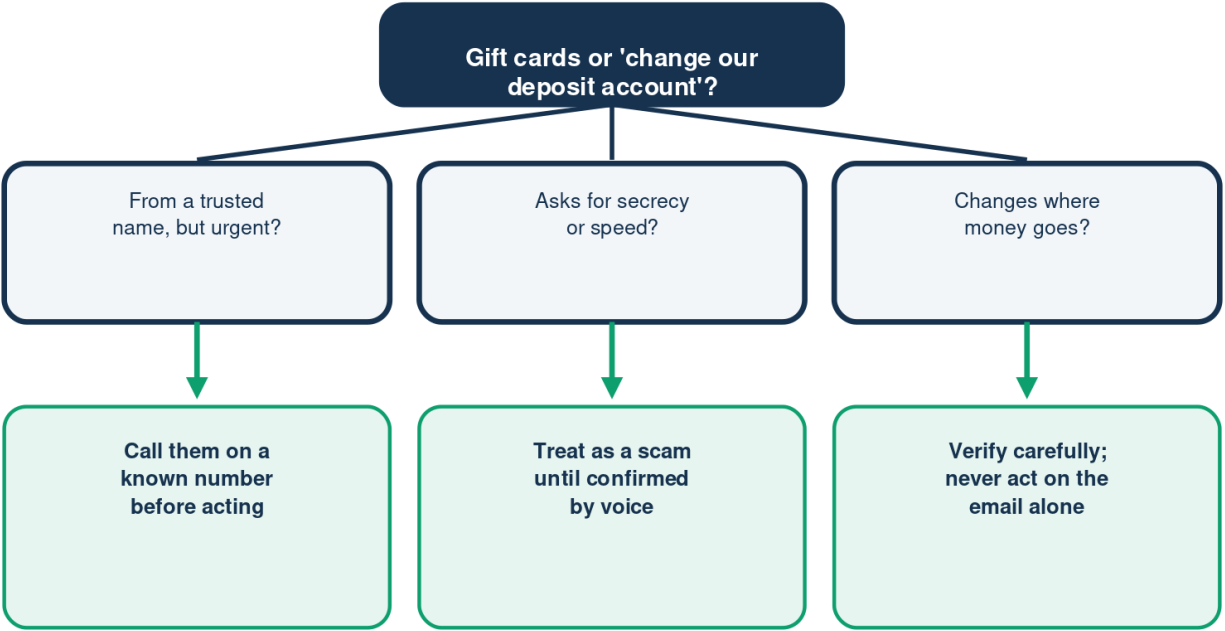
Least privilege, role by role

	Role	What they see
Office staff	Day-to-day	Most systems
Treasurer	The money	Giving, donations
Program volunteer	Their area	That program only
Communications	Outreach	Newsletter, website

Start each role small; add access only when truly needed.

A Surprise Money Request Arrives

Protect generous people from fraud



Real leaders rarely ask for gift cards by surprise email.

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