



An Extended Guide · No. 2080

Locking Down Microsoft 365 Sign-Ins: Security Defaults & Admin Protection

The free switch that blocks most
account takeovers, in plain English

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. In Microsoft 365, there's a free setting that does most of that work for you at once — it's called Security Defaults, and turning it on is the single highest-value hour you can spend on your email and files.

Let's lock down your Microsoft 365 sign-ins

If your business runs on Microsoft 365 — Outlook email, Word and Excel, Teams, OneDrive — then your sign-ins are the front door to everything. The good news is that Microsoft gives you a free, built-in way to block most account takeovers. This guide walks you through it in plain English.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. I've spent 30+ years helping small businesses with their technology, in plain language. You don't need to be an IT pro to do this — you need to know which switch to flip and why, and I'll show you.

One honest heads-up up front: Microsoft renames and moves these settings fairly often. I'll give you the names and the path as they stand at the time of writing, but if what you see on screen doesn't match exactly, that's normal — look in your current admin center or give me a call.

★ I can turn this on with you in one short visit

Flipping on Security Defaults and checking your admin accounts is usually a quick job, and I'll make sure nobody gets locked out in the process. Call or text me at (330) 200-8042.

The whole guide, on one page

If you remember only these things, your Microsoft 365 is far safer than most.

- ❑ **Security Defaults** is a free baseline in Microsoft Entra ID (formerly Azure AD) that blocks most account takeovers.
- ❑ It forces **everyone to set up MFA**, requires MFA for admins, and **blocks legacy (old, insecure) sign-in methods**.
- ❑ Turn it on in the **Microsoft Entra admin center** — path as of writing below, but confirm in your current admin center.
- ❑ Protect your **Global Administrator** account above all others, and keep a **break-glass admin** for emergencies.
- ❑ Don't do daily email in the Global Admin account — keep admin separate from everyday accounts.
- ❑ **Conditional Access** is the more flexible paid option; you use Security Defaults **or** Conditional Access, not both.

! Most break-ins are just a stolen password

Account takeovers overwhelmingly start with a password that got guessed, reused, or phished — not fancy hacking. Security Defaults shuts the door on almost all of it by requiring a second step. That's why it's the first thing to turn on.

What Security Defaults actually does

Let's demystify the name. Security Defaults is just a single free switch that turns on a bundle of sensible protections at once.

Microsoft 365 sits on top of an identity system now called **Microsoft Entra ID** (you may remember it as Azure AD). That's the part that handles who's allowed to sign in. **Security Defaults** is a free baseline you can switch on there, and it's designed exactly for small businesses that don't have an IT department.

When you turn it on, it does three big things automatically:

- **Requires everyone to register for MFA** — a second sign-in step using the Microsoft Authenticator app — within roughly 14 days.
- **Requires MFA for administrator accounts**, which are the ones attackers most want.
- **Blocks legacy authentication** — old sign-in methods that can't do MFA and are a favorite way in for attackers.

✓ One switch, several protections

You don't have to configure each of those pieces separately. Security Defaults is Microsoft's 'just make it safe' button for small businesses — flip it once and the bundle is on.

Why that second step matters so much

At the heart of Security Defaults is MFA. Here's why it does more than anything else you could turn on.

MFA — multi-factor authentication, also called two-step sign-in — means a password by itself isn't enough to get in. There's a second step: usually a tap or a code from the Microsoft Authenticator app on your phone. So even if someone steals or guesses a password, they still can't sign in without that second step sitting in your pocket.

Almost every Microsoft 365 account takeover I hear about comes down to a password that leaked — reused from another site, typed into a fake login page, or simply guessed. MFA defeats nearly all of that in one move, which is why insurers now treat it as a baseline requirement and why Microsoft builds it right into Security Defaults.

! A password alone is not a lock anymore

Treat any account that has only a password as effectively unlocked. The whole point of Security Defaults is to make sure every account — yours, your staff's, and especially your admins' — has that second step.

How to turn on Security Defaults

Here's the path as it stands at the time of writing. Microsoft moves these menus, so if yours looks different, confirm in your current admin center.

- Sign in to the **Microsoft Entra admin center** with your Global Administrator account.
- Go to **Identity > Overview > Properties**.
- Find **Manage security defaults**.
- Set it to **Enabled** and save.

Once it's on, every user will be prompted to set up the Microsoft Authenticator app the next time they sign in, and they have about 14 days to finish. It's worth giving your team a heads-up so the prompt doesn't surprise anyone — a quick 'you'll be asked to set up an app on your phone, it's expected' goes a long way.

✓ Settings move — the idea doesn't

If 'Identity' or 'Properties' isn't where this guide says, look for anything named security defaults in your admin center, or search its help. The location may change; the switch itself is the thing you're after.

What your team will see afterward

Turning it on is quick; knowing what happens next keeps it from feeling disruptive.

The first time each person signs in after you enable Security Defaults, they'll be walked through setting up the Authenticator app — install it, scan a code, done. After that, signing in means entering their password and then approving a prompt on their phone. On trusted devices they won't be asked every single time, so it's not as constant as people fear.

A couple of older things may stop working: ancient email programs or devices that can't do MFA (that's the 'legacy authentication' being blocked, and that's a good thing). If something you rely on breaks, don't panic — it usually means that thing was using an insecure sign-in method and needs updating.

✓ Warn your team before, not after

The only real friction with Security Defaults is surprise. Tell everyone a day ahead that they'll set up a phone app at next sign-in, and the rollout goes smoothly.

Guard the Global Administrator account

Of all your accounts, one deserves the most protection: the Global Administrator.

The Global Administrator is the account that can change everything in your Microsoft 365 — add and remove people, read anyone's mail, reset passwords, and change security settings for the whole organization. If an attacker gets that one account, they get the keys to the kingdom. So it needs the strongest protection you have.

That means MFA on it without exception, a strong and unique password, and — importantly — **not using it as your everyday email account**. Sign in to the Global Admin account only when you need to make an admin change, and read your daily mail from a normal account. Our guide 'Who's the Admin?' goes deeper on keeping admin and everyday accounts separate.

! Microsoft is tightening admin sign-in security

Microsoft has been rolling out mandatory MFA for signing in to its admin centers, because admin accounts are the prize target. Getting MFA on your Global Admin now means you're ahead of the requirement, not scrambling to catch up.

Keep a 'break-glass' admin for emergencies

Locking things down raises a fair worry — what if I get locked out? The answer is a break-glass account.

A **break-glass admin** is a spare Global Administrator account you create, write down, and lock away — like the little hammer behind glass by a fire exit. You never use it day to day. It exists for the moment your regular admin is unavailable, locked out, or an account gets compromised and you need a clean way back in.

Give it a strong unique password, protect it with MFA, and store its login somewhere truly safe and separate — a sealed envelope in a safe, or your password manager's most protected entry. Make sure the owner knows where it lives. And test it a couple of times a year so you know it still works before you ever need it.

✓ Set it up before you turn the locks tighter

Create your break-glass account as part of locking down, not after a lockout. It's cheap insurance, and the peace of mind lets you tighten everything else with confidence.

Security Defaults or Conditional Access — not both

You may hear about a second option called Conditional Access. Here's how to know which one is right for you.

Conditional Access is a more flexible, rule-based way to require MFA — for example, 'ask for MFA only when someone signs in from outside the country.' It's powerful, but it requires a paid add-on (Microsoft Entra ID P1 or P2) and someone to set up and maintain the rules. You use **Security Defaults OR Conditional Access, not both at the same time.**

For most small businesses, Security Defaults is the right answer: it's free, it's on in minutes, and it covers the essentials. Conditional Access makes sense once you're larger, have specific needs, and have the paid licensing and someone to manage it. There's no prize for the fancier option if the free one already protects you.

	Security Defaults	Conditional Access
Cost	Free	Paid (P1/P2)
Setup	One switch	Rules to build
Best for	Most small shops	Larger/complex
Can run together?	No	No

Two kinds of Microsoft 365 shops

The free baseline suits almost everyone, but the right choice depends a little on how big and how complex your setup is.

If you're a small shop on basic Microsoft 365

A handful of users, standard email and files, no special sign-in rules. This is exactly who Security Defaults was built for.

- Turn on **Security Defaults** — free, fast, and it covers the essentials.
- Get everyone onto the Microsoft Authenticator app in the first two weeks.
- Protect your Global Admin and set up a break-glass account.
- You almost certainly don't need Conditional Access or paid add-ons.

If you're larger or have special needs

More users, a mix of locations or devices, or a requirement to allow access only under certain conditions. You may outgrow the one-size switch.

- Consider **Conditional Access** if you need rules like location- or device-based MFA — but remember it's paid and needs managing.
- You still can't run both at once, so plan the switch deliberately.
- An insurer or a framework may ask for specific controls Conditional Access can enforce — confirm what's actually required.
- Even then, keep the fundamentals: MFA everywhere, protected admins, a break-glass account.

★ Not sure which one you need?

Tell me how many people you have and how your Microsoft 365 is set up, and I'll tell you honestly whether free Security Defaults is plenty or whether you'd benefit from more — no upsell, since I don't sell the licenses. Call (330) 200-8042.

A plain-English word about the Authenticator app

The second step is simplest with the Microsoft Authenticator app. Here's what your team should know.

The Microsoft Authenticator is a free app on each person's phone. After it's set up, signing in means entering your password and then either tapping 'Approve' on a notification or typing a short number the screen shows you. It's quick once people get used to it — a second or two, not a hassle.

- Each person installs the app on their own phone and links it to their account once.
- After that, sign-in is password plus a tap or a short number.
- If someone changes phones, they re-register the app — a good reason to have a break-glass admin who can help.
- Approve prompts **only** when you're the one signing in; an unexpected prompt can mean someone has your password.

! Never approve a prompt you didn't start

Attackers sometimes spam approval prompts hoping you'll tap 'Approve' to make them stop. If you get a sign-in prompt you didn't trigger, deny it and change that password — it means someone already has it.

For your most valuable accounts, go stronger

A phone-app tap is great. For your admins and highest-value accounts, there's a step better.

Phishing-resistant sign-in — **passkeys** and hardware **security keys** — is even stronger than an app prompt, because it's bound to the real website. A fake login page simply can't capture anything it could reuse. For a Global Administrator or any account that controls a lot, that extra protection is well worth it.

You don't have to roll this out to everyone at once. A sensible plan is to put the strongest protection on the few accounts that matter most — your admins — and the standard app-based MFA on everyone else. Our guide on passkeys and security keys walks through exactly how, and who to start with.

✓ Match the lock to the value behind the door

Your front-desk login and your Global Admin login don't carry the same risk, so they don't need the same lock. Standard MFA for everyday accounts, phishing-resistant keys for the powerful ones.

A few rules for admin accounts

Security Defaults protects everyone, but your admin accounts deserve a little extra discipline.

- Keep the number of Global Administrators **small** — often the owner and one trusted backup is plenty.
- Don't read everyday email in a Global Admin account — keep admin separate from daily work.
- Give each admin their **own** admin account; never share one admin login among several people.
- Protect admins with the strongest MFA you can — ideally a security key or passkey.
- Keep a written list of who holds admin rights, and review it a couple of times a year.

✓ Fewer keys, fewer worries

Every extra Global Admin is another password a thief could steal and another account you must guard. In a small shop, keep that circle as tight as you can — it's less to protect and less that can go wrong.

A few more settings worth a look

Once Security Defaults is on, these quick checks round out your sign-in security.

None of these are as urgent as MFA, but each closes a small gap. The exact names and locations may differ in your admin center, so treat these as things to look for rather than exact clicks.

- **Recovery details:** make sure the admin account's recovery email and phone are current and under your control, not a former employee's.
- **Sign-in activity:** Microsoft 365 can alert you to unusual sign-ins — know where those alerts go.
- **Old accounts:** disable accounts for people who've left (see our offboarding guide) so they can't be used against you.
- **Shared mailboxes:** make sure a shared mailbox isn't a sneaky way to sign in without MFA.

✓ Don't let the extras delay the main thing

If you only have time for one thing today, it's Security Defaults and protecting your Global Admin. Come back for these finishing touches when you can — they're the polish, not the foundation.

If you run both Microsoft and Google

Plenty of small businesses have a foot in both camps. The good news: the ideas carry straight across.

Maybe your email is on Microsoft 365 but a side of the business uses Google Workspace, or you're mid-switch between them. The sign-in principles are identical: require a second step for everyone, protect the top admin account, keep admin separate from everyday accounts, and keep a break-glass admin. Only the menu names differ.

If you use Google Workspace too, our companion guide 'Locking Down Google Workspace' covers the same job on that side — turning on 2-Step Verification, enforcing it, and protecting the super-admin. Wherever your mail lives, the second step is the thing that matters most.

★ Running a mix? I handle both

Lots of the offices I help have one foot in Microsoft and one in Google. I can lock down the sign-ins on both sides in a single visit so you're not juggling two different to-do lists. Call (330) 200-8042.

The mistakes that leave the door cracked

Even with Security Defaults available for free, a few habits quietly undercut it. Now you'll spot them.

- **Leaving Security Defaults off** because 'we'll get to it' — the most common and costly delay.
- **No MFA on the Global Admin**, which is the one account that most needs it.
- **Using the Global Admin as a daily mailbox**, exposing the most powerful account to everyday phishing.
- **No break-glass account**, so one lockout becomes a crisis.
- **Approving MFA prompts you didn't start**, handing an attacker the second step.
- **Turning on Conditional Access without the paid licensing or anyone to manage it**, and losing the simple protection you had.

! The free switch only helps if it's on

The single biggest Microsoft 365 mistake I see isn't a wrong setting — it's a protection left switched off. Security Defaults costs nothing and takes minutes. Don't let it sit undone.

A simple lockdown plan

Here's the whole job in a sensible order, biggest wins first.

- ❑ Confirm who your **Global Administrator(s)** are and that the count is small.
- ❑ Create and lock away a **break-glass admin** account.
- ❑ Turn on **Security Defaults** in the Microsoft Entra admin center.
- ❑ Give your team a heads-up and get everyone onto the Authenticator app within two weeks.
- ❑ Move the Global Admin out of daily email use.
- ❑ For admins, add a security key or passkey for the strongest protection.

Work top to bottom and you'll have the essentials done in an afternoon. If any step gives you pause — especially avoiding a lockout — that's exactly the kind of thing I'm glad to handle with you on a call or a visit.

How to know it actually took effect

A few quick checks confirm the protection is really on — not just intended.

- Sign out and back in as a normal user — you should be asked for the second step.
- Confirm each person, including you, has set up the Authenticator app.
- Try signing in to the Global Admin account — it should demand MFA every time.
- Confirm your break-glass account's login and MFA both work.
- Check that your daily email is **not** the Global Admin account.

✓ Test it the way a thief would

The simplest proof is to try signing in with just a password. If Microsoft 365 stops you and insists on the second step, it would stop an attacker with a stolen password in exactly the same way.

Keeping it current over time

Sign-in security isn't set-and-forget. A light yearly touch keeps it solid as things change.

A couple of times a year, confirm your admin list is still short and correct, that MFA is on for everyone (including new hires), that recovery details are current, and that your break-glass account still works. When someone leaves, disable their account promptly — our offboarding guide makes that a same-day habit.

Also keep half an eye on Microsoft's own changes. They regularly tighten defaults and move settings around, and they've been expanding where MFA is required. When a prompt or a new requirement appears, it's almost always pushing you toward something safer — go with it rather than looking for a way around it.

✓ Pair it with your other yearly checks

This review sits naturally alongside your backup test, your admin-account review, and your insurance renewal. Doing them together makes one tidy security habit you won't forget.

The essentials, in one view

Keep this handy — it's the whole job summarized.

Step	What it does	Priority
Security Defaults	Free MFA baseline	Do first
Protect Global Admin	Guard the keys	Do first
Break-glass admin	Avoid lockout	Do early
Keys/passkeys	Stronger admin MFA	Soon after
Review and offboard	Keep it current	Ongoing

★ **Want it done right, without the lockout worry?**

I'll turn on Security Defaults with you, get everyone onto the app, protect your admins, and set up a break-glass account so nobody's ever stuck. Call or text (330) 200-8042.

Common Questions

The questions I hear most from owners locking down Microsoft 365.

Q: Is Security Defaults really free?

Yes. It's a free baseline built into Microsoft Entra ID (formerly Azure AD) and included with Microsoft 365. The paid option is Conditional Access, which most small shops don't need.

Q: Will MFA annoy my team every single time they sign in?

Less than people fear. On trusted devices you won't be prompted constantly — it's a tap or a short number now and then. A day's heads-up before you turn it on makes the rollout smooth.

Q: What if someone loses their phone with the Authenticator app?

They re-register the app on a new phone, and an admin can help. This is exactly why you keep a break-glass admin account — so a lost phone is an inconvenience, not a lockout.

Q: Should I use Security Defaults or Conditional Access?

For most small businesses, Security Defaults — it's free, fast, and covers the essentials. Conditional Access is the flexible paid option for larger or more complex setups, and you can't run both at once.

★ Still have a question?

There's no silly question here. Call or text me at (330) 200-8042 and I'll give you a straight, plain-English answer — and I don't sell Microsoft licenses, so it's just honest advice.

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 locking down your Microsoft 365 sign-ins 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.

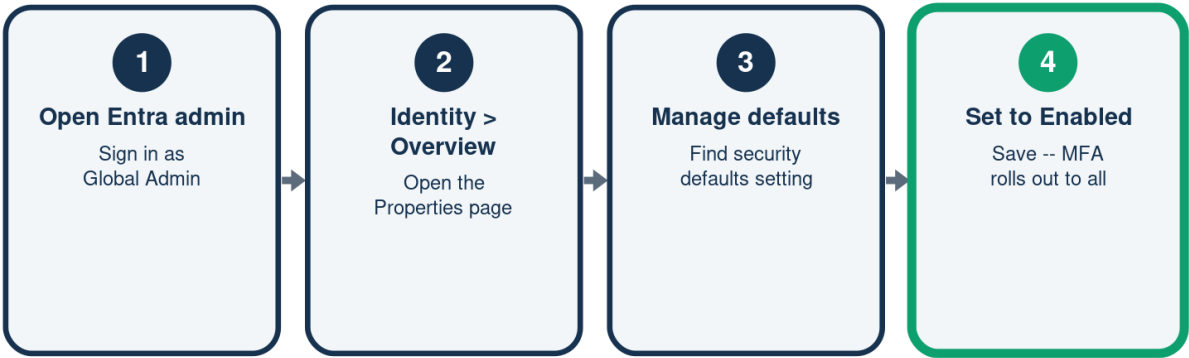
When you'd rather have a hand, that's exactly what I do. I come to your business, work at your pace, and never make you feel rushed or silly for asking. A first visit is a flat \$99, and for the parts that don't need me on-site I can often help right on your screen for \$49. Every visit comes with a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

Turning On Security Defaults

The path as of writing -- confirm in your admin center



Give your team a heads-up; they set up Authenticator within ~14 days.

Defaults vs. Conditional Access

Most small shops want the free one

	Security Defaults	Conditional Access
Cost	Free	Paid (P1/P2)
Setup effort	One switch	Rules to build
Best for	Small shops	Larger/complex
Run both at once	No	No

You use one or the other -- not both at the same time.

How Hard to Lock Each Account

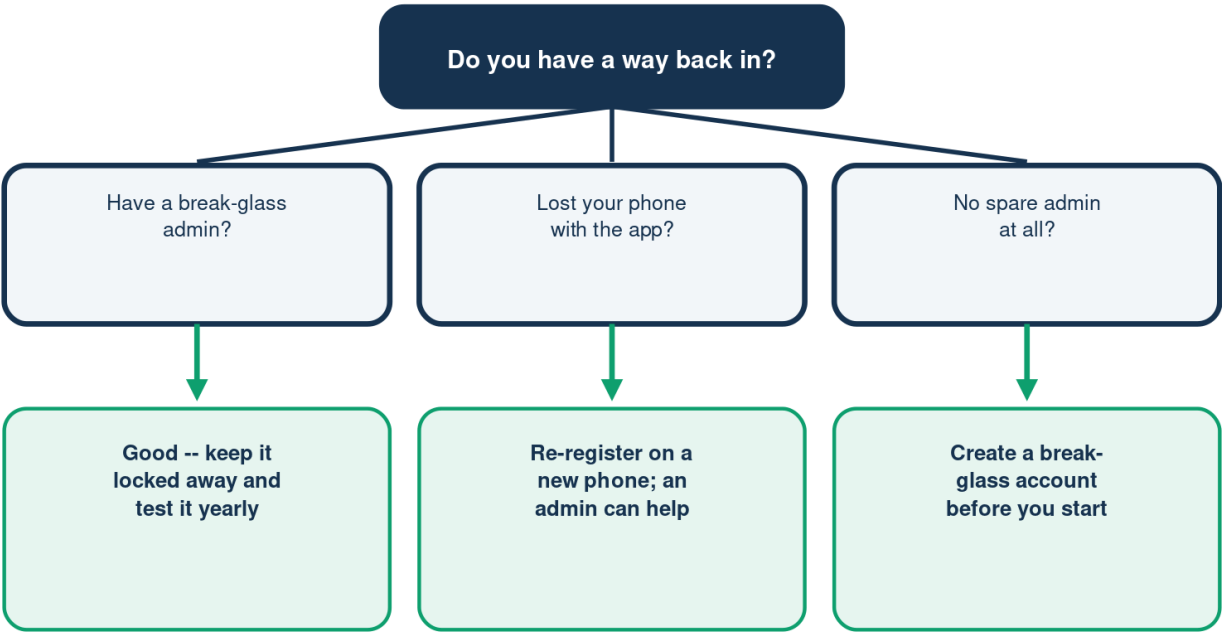
Match the lock to what's behind the door

	Protection	How often used
Everyday user	MFA via app	All day
Global Admin	Key or passkey	Rarely
Break-glass admin	MFA, locked away	Emergencies
Daily mailbox	Not the admin	All day

Standard MFA for everyone; phishing-resistant keys for admins.

Worried About Getting Locked Out?

Set the safety net before you tighten the locks



Never tighten sign-in security without a tested way back in.

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