



An Extended Guide · No. 2087

Vendors & Remote Access: Who Can Get Into Your Systems?

List who can reach you, remove what you don't use, set simple rules

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. There's one more door worth checking that owners almost always forget: the people and tools outside your business who can already reach your computers from somewhere else.

Who can get into your systems right now?

It's a simple question with a surprising answer. Most small businesses have handed out more ways in than they realize — to an IT helper, a software company, an old web designer, a screen-share app — and they've never once written them all down. This guide helps you do exactly that, calmly.

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 the way trouble gets in is rarely a Hollywood hacker. It's far more often a forgotten login that still works, or a remote-support tool left switched on.

So we'll do three plain things: make a list of everyone and everything that can reach your systems from outside, remove the ones you no longer use, and set a few easy rules for the remote-support tools you keep. No jargon, no judgment — just a tidy front door.

★ I'll help you find every way in

If you're not sure who still has access — or how to even check — that's a normal place to be, and it's exactly the kind of thing I help with. We can walk through it together in one visit. Call or text me at (330) 200-8042.

The whole guide, on one page

If you remember only these things, you'll close most of the risk that outside access creates.

- ❑ Make a **list** of everyone and everything that can reach your systems from outside — people and tools both.
- ❑ **Remove** any access you no longer use. An unused login is a door nobody's watching.
- ❑ Require **MFA** (a second sign-in step) on every kind of remote access, including your vendors'.
- ❑ Give each vendor their **own** login — never a shared account everyone passes around.
- ❑ Turn remote-support tools **off** when you're not in a session, and only turn them on when you start one.
- ❑ Before you let anyone in, **confirm who they really are** — a surprise 'support' call is a classic scam.

! The access you forgot about is the dangerous one

The logins that cause trouble aren't the ones you use every day — they're the ones you forgot existed: the developer who built your site five years ago, the trial software you stopped using, the shared password three people still know. Finding them is half the battle.

Why outside access is a favorite way in

It helps to understand why crooks love vendor and remote access so much — because it shows you where to look.

Every person or tool that can reach your systems from outside is another doorway. You lock your own front door out of habit, but these side doors were often propped open months or years ago and never checked again. A crook doesn't need to break your lock if a forgotten key still fits.

Remote access is attractive for a second reason: it's quiet. Someone signing in through a legitimate support tool or a vendor's account doesn't look like an attack — it looks like normal business. That's why the fix isn't fancy software; it's knowing exactly who should be coming through each door and slamming shut the ones nobody uses.

None of this means your vendors are the problem. Most are honest and helpful. The risk is simply that the more doors exist, the more there are for someone to slip through — so fewer, well-watched doors is the goal.

✓ Think of it as a key audit

If you handed out physical keys to your shop over the years, you'd eventually want to know who still has one. Remote access is the same — it's just that the keys are invisible until you write them down.

Step one: write down who can get in

You can't protect what you can't see. The first job is simply a list — and it's more satisfying than you'd think.

Sit down with a notepad or a simple document and write a line for every outside person or tool that can reach your computers, your email, your files, or your website. Don't worry about being perfect; you can add to it as you remember things. The point is to get them out of your head and onto paper where you can decide about each one.

Here are the usual suspects to jog your memory. Most businesses have more of these than they expect:

- Your **IT provider** or computer-repair person, and any tool they use to connect to you.
- **Software vendors** whose programs you log into, or who log into your systems to support them.
- The **web developer** or marketing company who built or manages your website — even if it was years ago.
- **Remote-support tools** — screen-share and remote-control apps on your machines.
- **Bookkeepers, payroll, or point-of-sale** services with a login to your money systems.
- Anyone who has your Wi-Fi password or a **VPN** connection into your office.

★ A list like this is a great first visit

Building this list is often the first thing I do with a new business. In an hour or two we can usually capture every way in and flag the ones that look stale. Call (330) 200-8042 and we'll start your list.

What 'access' actually means

'Access' is a vague word. Here's the plain-English version of the kinds you're looking for, so none slip past you.

Kind of access	What it lets them reach
A login to a service	Your email, files, or an app — as if they were you or a staff member
Remote-control software	The actual screen and keyboard of a computer, from anywhere
Admin or 'owner' rights	The power to change settings, add users, or remove protections
A VPN or network tunnel	A path into your office network as if they were sitting there
Website / hosting login	Your public site, and sometimes the customer data behind it

The ones that deserve the most attention are admin or owner rights and remote-control software, because they can do the most damage if misused or hijacked. Our guide on admin accounts goes deeper on keeping those powerful logins separate and protected.

✓ **Note what each one can reach**

Next to each line on your list, jot what that access actually touches. 'Can see email' is very different from 'can change everyone's passwords' — and knowing which is which tells you where to be strictest.

Step two: remove what you don't use

Now the satisfying part. Every door you can close is one fewer to worry about for the rest of time.

Go down your list and ask one question about each entry: do we still actually use this? If a vendor's contract ended, if you stopped using a piece of software, if the web developer finished the job two years ago — their access should be gone. Don't leave it 'just in case.' A login nobody uses is a login nobody is watching.

When you're not sure, the safe move is to remove the access and see if anything breaks. It's far easier to turn access back on for someone you trust than to discover, after a break-in, that a forgotten account was the way in. Removing access the day a relationship ends is the same tidy habit as offboarding an employee — our offboarding guide walks through that.

! The old web developer is the classic example

The single most common forgotten door I find is the person or company who built the website long ago. Their login often still works, still has full control, and nobody has thought about it in years. Make a point of checking that one specifically.

Require a second sign-in step on every way in

For the access you keep, this is the single most valuable rule — and it applies to your vendors too.

MFA — multi-factor authentication, also called two-step or two-factor sign-in — means a password alone isn't enough to get in. There's a second step: a code from an app, a tap on a phone, or a security key. It's the one thing that stops a stolen or guessed password from becoming a break-in, and it matters most on the doors that reach your systems from outside.

So require MFA on every kind of remote access: your own remote logins, your remote-control tools, your VPN, and — importantly — your vendors' access too. It's fair and normal to ask an IT provider or software company whether they use MFA to connect to you. A good one will say yes without hesitating.

! A vendor without MFA is a borrowed risk

If a vendor can reach your systems and their account gets stolen, the break lands on you. Insisting that everyone who touches your systems uses MFA — your people and theirs — is one of the highest-value rules you can set, and it costs nothing. Our Microsoft 365 and Google Workspace guides show how to turn it on.

Give each vendor their own login

Shared accounts feel convenient. They're also the reason nobody can ever tell who did what.

It's tempting to create one 'support' login and let every vendor and helper use it. Please don't. When everyone shares one account, you lose the two things that make access safe: you can't tell who signed in, and you can't cut off one vendor without disrupting all the others.

Instead, give each outside party their own named login. That way the records show exactly who connected and when, you can turn off a single vendor the moment you part ways, and nobody has to pass a password around by email or text — which is how shared passwords leak in the first place.

Shared login	Unique login per vendor
Can't tell who did what	Records show exactly who
Remove one, break all	Remove one, others fine
Password passed around	No shared secret to leak

✓ **Name the account for the vendor**

Call it what it is — 'AcmeIT-support,' not 'user2.' When a login's name tells you who it belongs to, your yearly review takes minutes and nothing mysterious lingers.

Turn remote-support tools off when you're not using them

A screen-share tool left running all the time is a door left standing open all night. It only needs to be open during the visit.

Remote-support tools let someone see and control your screen from elsewhere — wonderful when your IT person is fixing something, risky when it sits switched on and unattended for weeks. The simple rule: the tool is off by default, you turn it on when a session starts, and it goes back off when the work is done.

Many of these tools can be set so a session only works when you click to allow it, with a code that's good just for that visit. That's far safer than a tool that lets anyone with the password connect at any hour. If you're not sure how yours is set, that's worth checking — or ask me.

- Keep the tool **off** or in 'ask me first' mode unless a session is live.
- Use a **one-time code** per session where the tool offers it, not a standing password.
- **Watch the screen** during the session so you can see what's being done.
- When the work ends, confirm the session has **closed** and the tool is off.

! An always-on remote tool is an open invitation

If a remote-control tool is set to let anyone connect any time with just a password, treat that as a problem to fix today. Those standing connections are exactly what crooks hunt for.

A solo shop and a team watch different doors

The idea is the same for everyone — know who can get in and close what you don't use — but where the risk hides depends on how your business runs.

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

You probably have only a handful of outside connections, which is good news: you can likely list and tidy them all in one sitting. Your biggest risks are usually a forgotten website login and a remote-support tool left on.

- Check the one or two vendors who've ever connected, plus whoever built your website.
- Set your remote-support tool to 'ask me first' so nothing connects without you.
- Turn on MFA for your own email, files, and any remote login — that covers most of your exposure.
- Because it's just you, confirming who's really calling before a session is entirely in your hands — slow down and verify.

If you have employees and several vendors

More people and more vendors means more doors and more chances one gets forgotten. The questions about shared logins, who has admin rights, and cutting off access when a vendor leaves all apply squarely to you.

- Give every vendor their own named login — no shared 'support' account the whole team passes around.
- Keep a written list of vendor access and review it on a set schedule, not just when something feels off.
- Require MFA on your vendors' access as well as your staff's, and ask providers to confirm they use it.
- When a vendor relationship ends, cut their access the same day — the same habit as offboarding an employee.

★ Not sure which doors you've left open?

Tell me how your business runs — who helps with IT, who built your site, what you log into — and I'll help you map every way in and close the ones you don't need. Call (330) 200-8042.

Before you let anyone in, make sure they're really them

A friendly voice saying 'I'm from support and I need to fix something' is one of the oldest tricks there is. Verify first, always.

Crooks call and pretend to be your software company, your bank's tech team, or even your own IT provider, hoping you'll let them into your computer. They create urgency — 'your account is compromised, we need in right now' — because panic makes people skip the one step that would stop them: checking.

The rule is simple and it never fails you: don't grant a remote session to anyone who contacted you. If you didn't start the conversation, hang up and call the company back on a number you already have — from a past invoice, the back of a card, or their official website — never a number the caller gives you. Our guide on scam call-backs covers this verify-first habit in more detail.

! Real support does not cold-call to get into your PC

Legitimate companies don't phone you out of the blue demanding remote access to fix a problem you didn't report. If that call comes, it's a scam until you've proven otherwise by calling back on a known number. There's no rudeness in saying 'I'll call you right back.'

Write down a few simple remote-support rules

A short, written rule turns 'I think we do it this way' into something your whole team actually follows.

You don't need a thick policy. A half-page of plain rules, posted where your team can see it, is plenty. Writing it down matters because the person who answers the phone when a 'support' call comes in may not be you — and they need to know, in advance, what the rule is.

- ❑ We never grant a remote session to someone who contacted us — we call the company back on a known number first.
- ❑ Our remote-support tool stays off or in 'ask me first' mode unless a session is live.
- ❑ Every vendor uses their own login, and MFA is required on all remote access.
- ❑ We keep a list of who can get into our systems and review it on a set date each year.
- ❑ When a vendor relationship ends, we remove their access that same day.

✓ Tape it by the phone and the main computer

The rule only helps if it's visible at the moment someone's being pressured to say yes. A posted reminder gives whoever's at the desk permission to pause and verify.

A simple access log you can reuse

One tidy page answers the question 'who can get into our systems?' in seconds — forever.

Keep a single list, on paper or in a document, with a line for each outside person or tool that has access. It doesn't need to be fancy; it needs to exist and stay current. Here's what each line should capture:

- **Who** it is — the person, company, or tool.
- **What** they can reach — email, files, website, admin, and so on.
- **How** they get in — their own login, a remote tool, a VPN.
- **MFA on?** — yes or no, so gaps jump out at you.
- **Still needed?** — and the date you last confirmed it.

Update it whenever you add a vendor or end a relationship. With this one page current, both your yearly review and any insurance or security question become a quick, calm task instead of a scramble.

★ I'll help you build the log once

We can put this list together in a single visit, and I'll show you how to keep it up with almost no effort. After that it practically maintains itself. Call (330) 200-8042.

When a vendor or helper moves on

The end of a relationship is exactly when a forgotten login gets left behind. A clean handoff prevents that.

The day you stop working with a vendor, an IT helper, or a web company is the day to remove their access — not 'sometime soon.' People leave on good terms and bad, and either way a standing login outlives the relationship if nobody closes it. This is the same thinking as our offboarding guide for employees: cut access the same day.

If the vendor set things up for you, make sure you — not just they — hold the master logins before you part ways. You never want the only key to your website, your domain, or your email to walk out the door with a departing vendor. Our guide on hiring outside IT help covers exactly which keys the owner must always keep.

! Don't let the only key leave with them

Before any vendor relationship ends, confirm you can still get into everything they touched — website, domain, email, accounts. If the answer is 'only they can,' fix that first, while they're still cooperative.

Be careful what you hand a vendor the keys to

Some access is ordinary; some is the master key to everything. Treat the master keys with extra care.

A vendor who needs to update one app should get access to that app — not full administrator or owner rights over your whole system. The more powerful the access, the more damage it can do if that vendor's account is ever stolen or misused. Give each party the least access that lets them do their job, and no more.

This matters most for the truly powerful logins: the main administrator of your Microsoft 365 or Google Workspace, your domain registrar, your website host. It's fine for a vendor to help with these, but you should hold the master credentials and grant them their own, more limited access. Our guides on admin accounts and on hiring outside IT help go deeper on this.

✓ Least access is a kindness to everyone

Giving a vendor only what they need protects them too — if something goes wrong on a system they could never touch, they're plainly in the clear. Narrow access makes trust easier, not harder.

Your IT provider is a vendor too

The people who help you with technology hold some of the most powerful access of all — so the same rules apply to them.

A good IT provider will welcome these questions, not bristle at them. It's entirely reasonable to ask how they connect to you, whether they use MFA, whether each of their technicians has their own login, and how they'd hand things back if you ever parted ways. Those questions are a sign you're a careful client, not a difficult one.

If a provider resists giving you your own master credentials, or wants to be the only one who can get into your systems, treat that as a yellow flag worth a conversation. Our guide on hiring outside IT help lays out what to ask and what to keep control of — it pairs closely with this one.

★ I can help you interview or oversee an IT provider

Vetting an IT provider — or just double-checking the one you have — is squarely in my lane. I can sit in on the conversation and help you ask the right questions, without being your IT provider myself. Call (330) 200-8042.

Red flags worth acting on

A few patterns almost always mean a door needs attention. Spot these and you're ahead of most businesses.

- A remote-support tool that's **always on** and lets anyone connect with just a password.
- A **shared** login that several vendors or staff all use.
- A vendor or developer you **no longer work with** whose access was never removed.
- Any remote access **without MFA** — yours or a vendor's.
- A **surprise call** asking to get into your computer right now.
- A provider who won't let you **hold your own** master credentials.

! You don't have to fix them all today

Finding a few of these is normal, not a failure. Start with the two that matter most — turn off always-on remote tools and remove access for anyone you no longer work with — and work down the rest at your own pace.

Give the doors a check-up once a year

Access tends to pile up quietly. A short review on a set date keeps the list honest.

Pick a date you'll remember — your business anniversary, tax time, the start of the year — and spend a half hour going down your access log. For each line, ask the same two questions: do we still use this, and does it have MFA? Remove what's stale, fix any gaps, and date the review so you know it's current.

This is the habit that keeps everything else from unraveling. Without it, a tidy list slowly drifts out of date as vendors come and go. With it, you'll always be able to answer 'who can get into our systems?' with confidence — and that confidence is worth a great deal.

✓ Pair it with your other yearly check-ups

Fold this into the same sitting where you review your backups and your insurance answers. One tidy afternoon a year covers a surprising amount of your security.

Write down what you did

A little record now makes insurance questions, audits, and your own future reviews far easier.

When you remove access, turn on MFA, or set a remote-support rule, make a quick note of it with the date. If you ever fill out a cyber-insurance application, you'll be asked about remote access and MFA — and being able to point to your current access log and dated changes turns a stressful question into a simple one.

Store these notes with your other business papers and your access log, ideally somewhere that doesn't depend on the computers they describe. Think of it as the receipts proving your doors are watched.

✓ Your access log is most of the proof

A current, dated access log answers most of what an insurer or a security review will ask about outside access. Keep it current and you've already done the hard part.

Tools and settings change — confirm the current way

Remote-support apps and admin centers update their menus constantly. The idea stays the same even when the buttons move.

The names and locations of settings — where you turn on MFA, where a remote tool's 'ask me first' option lives, how you remove a vendor's login — change over time as software updates. Don't be thrown if a menu doesn't match a screenshot you saw. Look for the plain goal: a second sign-in step, a tool that's off by default, access you can remove.

When you can't find the right setting, check the tool's own current help pages, or ask someone you trust to confirm the current path. It's always better to verify than to assume a door is closed when it isn't.

★ Menus moved? That's what I'm for

If a setting isn't where you expected, don't fight it alone. I keep up with where these things live, and I'm happy to find it with you in a quick visit or on your screen. Call (330) 200-8042.

Common Questions

The questions I hear most from owners thinking about who can reach their systems, answered plainly.

Q: How do I even find out who has access right now?

Start with your own memory and your invoices — every vendor you pay is a candidate — then check each service's user or admin list for logins you don't recognize. It's a bit of detective work, and it's exactly the kind of thing I can do with you in a visit.

Q: Is it rude to ask my vendors whether they use MFA?

Not at all — it's a sign of a careful business. Anyone who can reach your systems should expect this question, and a good vendor answers it gladly. If a vendor is offended, that itself tells you something.

Q: Can I just use one shared login for all my helpers?

Please don't. A shared login means you can't tell who did what and can't cut off one vendor without disrupting the rest. Give each their own named login — it's safer and makes your records clear.

Q: Someone called saying they're from support and need into my PC. Now what?

Don't let them in. Hang up and call the company back on a number you already have — never the one the caller gave you. Real support doesn't cold-call demanding remote access. Our scam call-back guide covers this.

★ Still have a question about outside access?

There's no silly question here — this stuff is genuinely confusing until someone walks you through it. Call or text me and we'll sort it out together, in plain English. (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 who can get into your systems 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

Who Can Reach Your Systems?

The doors owners most often forget

Who or what		What to check
IT provider	Reaches everything	Own login? MFA?
Software vendors	Reach their app	Still in use?
Old web developer	Reaches your site	Remove if done
Remote-support app	Reaches the screen	Off when idle?

List every one, then remove what you no longer use.

Locking Down Outside Access

Four plain steps, start to finish



Then review the list once a year and keep it current.

Shared Login vs One Each

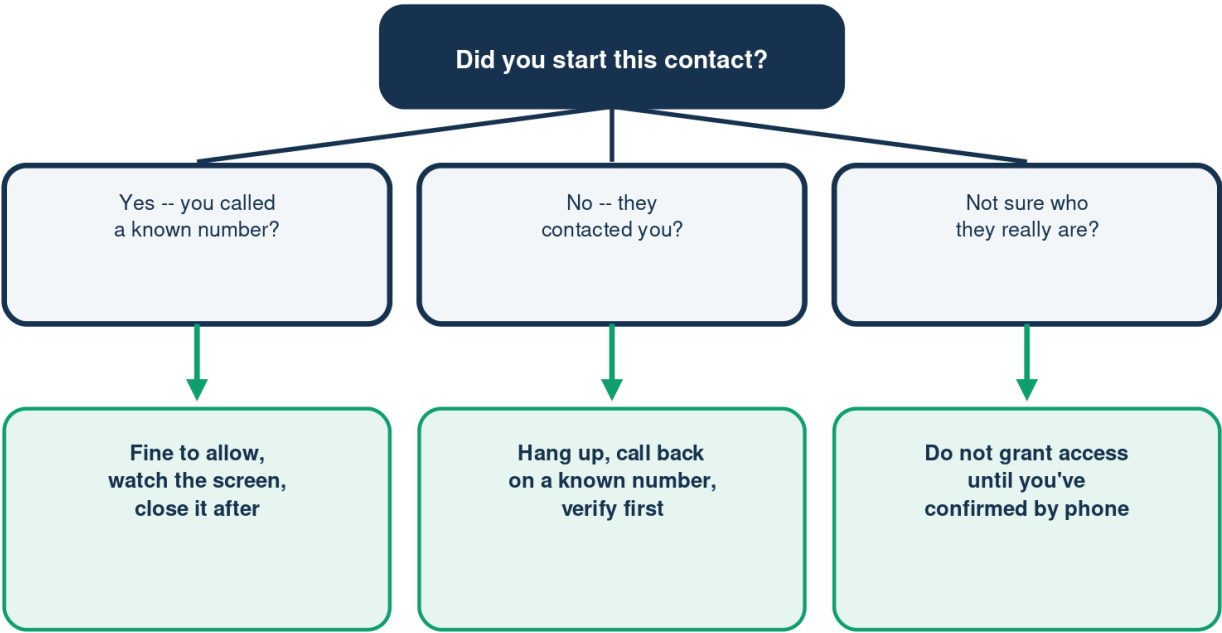
Why a login per vendor wins

	Shared login	One login each
Who did it?	No way to tell	Records show who
Removing one	Breaks everyone	Others unaffected
The password	Passed around	No shared secret

Give each vendor their own named login, with MFA on.

Someone Wants a Remote Session

Verify before you let anyone in



Real support never cold-calls demanding into your computer.

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