



An Extended Guide · No. 2078

Who's the Admin? Everyday Accounts vs. the Keys to the Kingdom

Separate admin power from daily work
so one bad click can't take everything

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. This guide adds one more habit to that list: keep the powerful 'administrator' account — the one that can change anything — separate from the account you use for everyday work, so one bad click can't hand over the keys to everything.

Who's the admin? Let's sort it out together

On every computer and every cloud service you use, some accounts can change everything — install software, add and remove people, rewrite security settings — and some can only do everyday work. Mixing those two powers into one account you use all day is one of the quietest risks a small business carries. The fix is simple and free.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. I've spent 30+ years helping folks and small businesses get comfortable with their technology, in plain language and at a kitchen-table pace. Nothing in here requires you to be technical — just willing to make one sensible change.

Think of it this way: you don't carry the master key to the whole building in your pocket every day just to unlock your own office. You keep the master key somewhere safe and carry the little key you actually need. Your computer accounts should work the same way.

★ I can set this up for you in one visit

Separating admin from everyday accounts takes me about an hour on a typical small-office setup, and I'll show you exactly how it works so it never trips you up. Call or text me at (330) 200-8042.

The whole guide, on one page

If you remember only these things, you've got the heart of it.

- ❑ Do your **daily work** — email, browsing, documents — in a **standard (non-admin) account**.
- ❑ Use **administrator rights only when you actually need them**, and then go back to your everyday account.
- ❑ In Microsoft 365 or Google Workspace, keep the top admin account (Global Administrator or super-admin) **separate** from the mailbox you read all day.
- ❑ Turn on **MFA** — a second sign-in step — for **every** admin account, no exceptions.
- ❑ Keep one safe **break-glass admin** account for emergencies, written down and locked away.
- ❑ The **owner** keeps the keys — never hand over the only copy of your admin login to anyone.

! An everyday account that can do everything is the danger

If the account you use all day also has full admin power, then a single stolen password or one bad click can reconfigure your whole setup or install malware with full rights. Separating the two is the single cheapest way to shrink that blast radius.

What an administrator account can actually do

Before you can separate the two, it helps to see plainly what each kind of account is allowed to do.

An **administrator account** is the account with the keys to the kingdom. It can install and remove software, create and delete other accounts, change security settings, and reach into places a normal user can't. A **standard account** can do everyday work — open programs, read email, write documents, browse the web — but can't quietly rewrite the machine or the service underneath it.

Task	Standard account	Admin account
Read email, write docs	Yes	Yes
Install new software	Asks permission	Yes
Add or remove users	No	Yes
Change security settings	No	Yes
Turn off protections	No	Yes

✓ **The point isn't to limit you — it's to limit a thief**

You lose almost nothing day to day by working in a standard account. But if someone hijacks it, they inherit only everyday powers, not the keys. That one difference stops a small problem from becoming a total takeover.

Why this is the keys-to-the-kingdom problem

Most break-ins don't start with fancy hacking — they start with a stolen password or a convincing email. What matters is what that account can do once someone's in.

Picture a scam email that talks someone into clicking a bad link or entering a password on a fake page. If that account is a plain everyday account, the damage is real but contained. If that same account is also a full administrator, the attacker now has your power: they can turn off protections, install whatever they want, lock you out, and reach every part of your business.

That's the whole reason to separate the two. You're not expecting to get fooled — nobody does — you're making sure that if anyone ever is, the account they catch can't reconfigure everything or install malware with full rights.

! One click should never cost you the whole business

When your daily account is also your admin account, every single email, link, and download you touch is a chance to hand over total control. Doing daily work in a standard account means a bad moment stays a bad moment — not a catastrophe.

The two-account idea on your own computer

This works the same on Windows and on a Mac: one account for every day, one for the rare moments you need the keys.

Your everyday account (standard)

This is where you live — email, documents, browsing, your day-to-day programs. It's a standard account, so if it ever gets hijacked, the attacker can't silently rewrite the machine. When a program genuinely needs admin power, the computer simply asks for the admin password.

Your admin account (used only when needed)

This is a separate account with full rights that you sign into only when you really need to — installing a program, making a system change. The rest of the time it sits unused, which is exactly the point. You type its password when prompted, do the one task, and go back to everyday work.

✓ You barely notice the difference

After the first day, the only change you'll feel is an occasional 'enter the admin password' box when you install something — a tiny speed bump that also stops a lot of sneaky software from installing itself.

Setting it up on Windows and Mac

The exact menus move around between versions, so I'll give you the plain shape of it — then check the current settings on your own machine or let me handle it.

- **Make a second account with admin rights.** Create a brand-new account, mark it as the administrator, and give it a strong, unique password you store in your password manager.
- **Change your everyday account to standard.** Once the new admin account works, switch your daily account down to a standard (non-admin) user. You'll still do everything you normally do.
- **Test it.** Sign in as your everyday account and try to install something — it should ask for the admin password. That prompt is the protection working.
- **Write down the admin login** and store it somewhere safe and separate, not on a sticky note on the monitor.

✓ Settings names change — confirm on your machine

Microsoft and Apple rename and move these screens regularly, so if the steps on your computer don't match word for word, that's normal. Look in your current account or user settings, or call me and I'll walk you through the version you actually have.

The same idea in Microsoft 365 and Google Workspace

Your cloud email and files have their own powerful admin account — and the same rule applies there.

In Microsoft 365, the top account is the **Global Administrator**. In Google Workspace, it's the **super administrator**. Either one can add and remove people, read anyone's mail, reset passwords, and change security for the whole organization. That is enormous power to be signing in and out of email with all day long.

So keep that top admin account **separate from your everyday mailbox**. Read your daily email as a normal user; sign into the admin account only when you need to make an admin change, then sign back out. If a phishing email ever catches your everyday login, it won't also be the login that controls the whole company.

- Give the top admin account its own name (not the one printed on your business cards) and its own strong password.
- Put **MFA** on it before anything else — it's the single most valuable account you own.
- Our guides 'Locking Down Microsoft 365 Sign-Ins' and 'Locking Down Google Workspace' walk through the exact settings for each.

Protect the one account that controls everything

If there's a single account worth guarding like the cash drawer, it's your top cloud administrator.

Because the Global Administrator or super-admin can change security for everyone, it's the account attackers want most and the one a mistake hurts most. Treat it as a tool you pick up for a specific job, not a chair you sit in all day. The less it's used, the less chance it's exposed.

A good habit for small offices: have no more than one or two people who hold top-admin access, keep a written list of exactly who they are, and review that list a couple of times a year. Fewer keys means fewer ways to lose one.

✓ Keep the admin count small on purpose

Every extra person with top-admin rights is another password a thief could steal and another account you have to protect. In a small shop, one owner and one trusted backup is often plenty.

Keep a 'break-glass' admin for emergencies

Separating accounts raises one fair worry: what if I get locked out? The answer is a break-glass account.

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

Store its login where you'd keep anything precious: a sealed envelope in a safe, or your password manager's most protected entry. Protect it with MFA too, and make sure at least the owner knows where it lives and how to use it.

✓ Check it once in a while

A break-glass account you can't actually get into isn't insurance. A couple of times a year, confirm the password still works and the MFA still lets you in — the same way you'd test a smoke detector.

What this looks like for you

The admin-versus-everyday idea works whether you're one person or a small team — but the day-to-day setup looks a little different.

If you're a solo operator or a tiny shop

With one or two people, you probably wear every hat, including admin. The goal is simply to stop living in the admin seat all day.

- Make yourself a standard everyday account and a separate admin account on your computer — both yours, just used for different things.
- In the cloud, read your daily mail as a normal user and keep a separate top-admin login for the handful of times you change settings.
- Create one break-glass admin and lock it away, since there's no colleague to let you back in.
- MFA on every admin account — it matters even more when it's all on you.

If you have employees

More people means it's worth being deliberate about who gets any admin power at all — and making sure nobody shares a single admin login.

- Give each person their **own** named account; never a shared 'office admin' login everyone uses.
- Most staff need only standard everyday accounts — hand out admin rights sparingly and only where the job truly requires it.
- Keep top cloud admin (Global Admin or super-admin) to the owner and one trusted backup, tracked on a written list.
- When someone leaves, named accounts make it clean to shut off — see our guide 'When an Employee Leaves.'

★ Not sure who should have what?

Tell me how your office runs and who does what, and I'll help you sort out which accounts need admin power and which don't — then set it up so it's tidy and safe. Call (330) 200-8042.

Put MFA on every admin account first

Separating accounts is step one; the next step is making sure the powerful ones can't be opened with just a password.

MFA — multi-factor authentication, also called two-step sign-in — means a password alone won't get you in. There's a second step: a code from an app, a tap on your phone, or a security key. On a normal account it's valuable. On an admin account it's essential, because that's the account a thief most wants.

- Turn on MFA for your top cloud admin (Global Admin or super-admin) before any other account.
- Turn it on for every other admin, including the break-glass account.
- For the most powerful accounts, a security key or passkey is stronger than a texted code — see our passkeys guide.

! An admin account without MFA is a door left unlocked

An administrator login protected by only a password is exactly what phishing and password-guessing are built to beat. If you do one thing after reading this guide, make it turning on MFA for your admin accounts.

Give people only the power they need

There's a tidy principle behind all of this, and it has a plain name: least privilege.

Least privilege just means each account gets the **least** power it needs to do its job — and no more. Not out of distrust, but because power you don't hand out can't be stolen or misused. A front-desk account doesn't need to install software or add users, so it shouldn't be able to.

- Start everyone at standard, and add power only when a real task requires it.
- If someone needed admin rights once for one task, take the rights back when the task is done.
- Review who has admin power a couple of times a year and trim anyone who no longer needs it.
- Treat 'they might need it someday' as a 'no' until the day actually comes.

✓ Less power, less to worry about

Every account without admin rights is one fewer account that can wreck your setup if it's hijacked. Least privilege isn't about control — it's about having fewer ways for a bad day to go very bad.

Why shared admin logins are the enemy

If several people sign into the same admin account, you've quietly undone most of the protection.

A shared login — one 'office admin' account everyone knows the password to — feels convenient, but it's a problem on every front. You can't tell who did what, you can't turn off one person's access without locking out everyone, and the password tends to live on sticky notes and in old emails where anyone can find it.

Individual, named accounts fix all of that. You know exactly who did what, you can grant or remove one person's access cleanly, and there's no shared secret floating around. It also makes the day someone leaves simple instead of a scramble.

! One shared password is one password away from trouble

The moment a shared admin password leaks — a former employee, a forwarded email, a reused password — everyone who used it is exposed and you may not even know. Give everyone their own login and the problem mostly disappears.

Whatever you do, the owner keeps the keys

This matters most when you bring in outside help — the owner must always hold the master keys.

It's perfectly fine to have an IT helper (even me) set up and manage your accounts. But you, the owner, should always keep your own copy of the top admin credentials — the Global Administrator or super-admin login — and the list of your critical accounts. Never let the only copy of the keys live with someone outside your business.

If a helper ever becomes unavailable, has a falling-out, or simply retires, you don't want your access to your own business walking out the door with them. Our guide on hiring outside IT help goes deeper on exactly what to keep in your own hands.

★ Good help hands you the keys, not the other way around

When I set things up, you keep the master logins — I'd never hold the only copy of your keys, and no one you hire should either. Want a second opinion on your current setup? Call (330) 200-8042.

What a normal day actually feels like

To make it concrete, here's how the two-account habit plays out in an ordinary workday.

Q: I sit down and open my email and the day's work.

You're signed into your standard everyday account — the one you use for everything. No admin power, so a bad link or attachment can't silently reconfigure your machine or your accounts.

Q: A program needs to update and asks for an admin password.

You type the admin password in that little box, the update runs, and you carry on. You never had to switch accounts — the computer just borrowed the admin power for one task.

Q: I need to add a new employee to Microsoft 365 or Google Workspace.

Now you sign into the separate top-admin account, add the person, and sign back out. The powerful account was open only for the few minutes you actually needed it.

✓ Power you pick up and put down

That's the whole rhythm: everyday work in a safe account, admin power borrowed briefly for a specific job, then set back down. It becomes second nature within a week.

The mistakes that undo all the good work

A few common habits quietly cancel out the protection. Now you'll spot them.

- **Doing daily work in an admin account** because it's 'easier' — this is the big one.
- **Reading everyday email in the Global Admin or super-admin account** — the most powerful account should not be your inbox.
- **Sharing one admin login** among several people instead of giving each their own.
- **Skipping MFA on admin accounts** because 'it's just me' — those are the accounts that need it most.
- **No break-glass account**, so one lockout turns into a crisis.
- **Handing the only copy of the keys to an outsider** and keeping none yourself.

! Convenience is how the keys end up in the wrong hands

Almost every one of these mistakes is made in the name of saving a few seconds. The seconds you save are tiny; the day you'd lose if an admin account is hijacked is not.

A simple plan to set this up

You don't have to do it all at once. Here's a sensible order that gets the biggest wins first.

- ❑ Put **MFA** on your top cloud admin account today — the single highest-value step.
- ❑ Create a separate everyday mailbox so you stop reading daily mail as the Global Admin or super-admin.
- ❑ On each computer, make a separate admin account and switch your daily account to standard.
- ❑ Create and lock away one **break-glass admin**.
- ❑ Replace any shared admin logins with individual, named accounts.
- ❑ Write down who holds admin rights, and confirm the owner has every master key.

Tackle one line a week and you'll be done within a month, with no disruption to your day. If you'd rather it be done in an afternoon, that's exactly the kind of visit I'm glad to make.

How to know you got it right

A few quick checks tell you the separation is really in place — not just intended.

- When you try to install software in your everyday account, you get a prompt for an admin password. (Good — that's the protection.)
- Your daily email inbox is **not** the Global Admin or super-admin account.
- Every admin account, including break-glass, asks for a second step at sign-in.
- You can name, off the top of your head, exactly who holds admin rights — and the list is short.
- The owner can open the master keys without anyone else's help.

✓ Test it the way an attacker would

The simplest proof is to sign in as your everyday self and try to do something powerful. If the system stops you and asks for the admin password, it would stop a thief in that same account too.

Keeping it tidy as your business changes

Accounts drift over time — people come and go, someone gets admin 'just for today' and it sticks. A light touch keeps it clean.

Put a short review on your calendar a couple of times a year. Walk the list of accounts and ask three questions: does this person still work here, do they still need the power they have, and is anyone sharing a login that should be individual? Trim anything that doesn't pass.

The same review is a natural moment to confirm MFA is still on for every admin and that your break-glass account still works. Ten minutes twice a year keeps small messes from becoming the thing that bites you later.

✓ Pair it with another yearly check-up

This review pairs naturally with your backup test and your insurance renewal. Doing the three together makes a tidy little security habit you won't forget.

The whole idea, in one table

Keep this handy — it's the plan on a single page.

Account	Use it for	How to protect it
Everyday (standard)	Daily work, email	MFA; no admin rights
Your admin account	Installs, changes	MFA; only when needed
Top cloud admin	Org-wide changes	MFA; keep separate
Break-glass admin	Emergencies only	MFA; locked away

Notice the pattern: MFA on everything, admin power kept separate and used sparingly, and the most powerful accounts touched least. That's the entire philosophy of this guide in one glance.

★ **Want me to build this for your office?**

I'll map your accounts to this table, set up what's missing, and leave you with a simple written list of who holds what. Call or text (330) 200-8042.

Common Questions

The questions I hear most about admin and everyday accounts, answered plainly.

Q: Isn't it a hassle to work in a standard account?

Not really. The only change you'll feel is an occasional prompt for the admin password when you install or change something — a couple of seconds that also blocks a lot of sneaky software.

Q: It's just me — do I really need two accounts?

Yes, and it's easy. Make yourself a standard everyday account and a separate admin account on your computer, and keep a separate top-admin login in the cloud. One person can hold several accounts; they're just used for different jobs.

Q: What if I lock myself out of the admin account?

That's exactly what the break-glass admin is for — a spare, locked-away admin login you can fall back on. Keep it written down safely and test it a couple of times a year.

Q: Can I just let my IT person be the admin?

They can manage things, but you the owner must keep your own copy of the master keys. Never let the only copy of your top admin login live outside your business — our guide on hiring IT help explains why.

★ 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 — no jargon, no sales pitch.

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 sorting out admin and everyday accounts 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

Everyday vs. Admin Account

Same person, two different jobs

	Everyday account	Admin account
Daily email and work	Yes	No
Install software	Asks password	Yes
Add/remove users	No	Yes
How often you use it	All day	Rarely

Work in the everyday account; borrow admin power only when needed.

Setting Up the Split

A calm order that gets the big wins first



One step a week and you are done within a month, with no disruption.

Admin in the Cloud

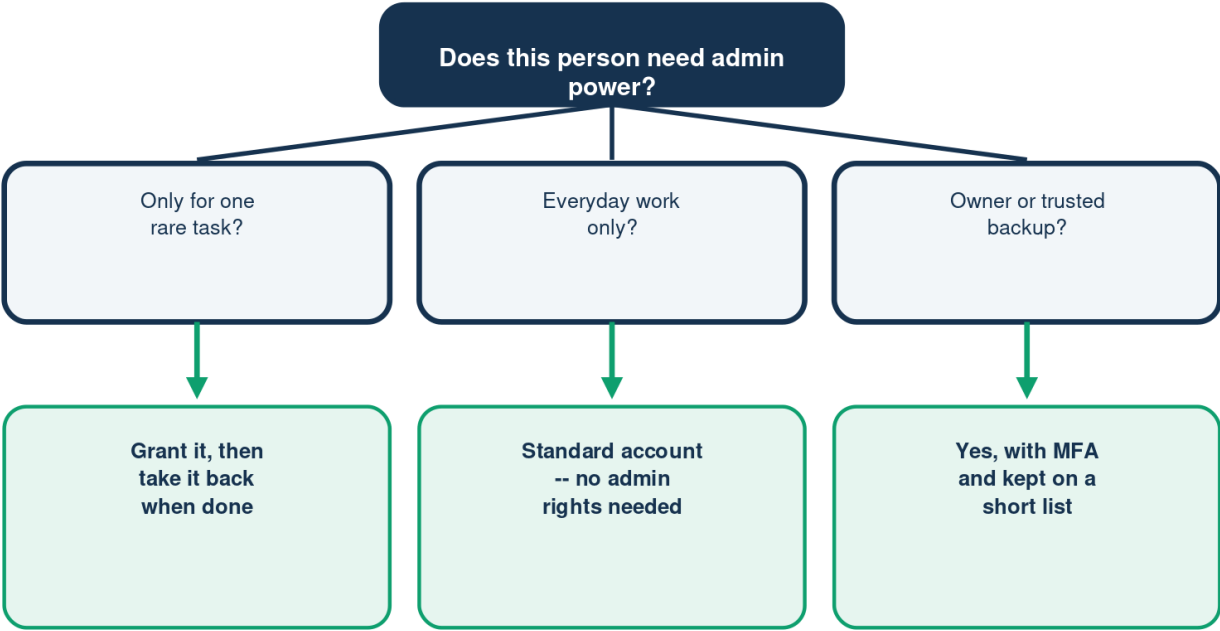
Keep the top account out of your inbox

	Everyday mailbox	Top admin account
Reads daily email	Yes	No
Changes org settings	No	Yes
Exposed to phishing	Lower risk	Keep it rare
Needs MFA	Yes	Yes, first

Global Admin and super-admin should never be your daily inbox.

Who Should Have Admin Rights?

When in doubt, the answer is standard



Power you don't hand out can't be stolen -- give the least that works.

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