BILL'S HOME TECH

Home & Small Business Tech Solutions

AN EXTENDED GUIDE · NO. 1992

Updated November 2026

Who Can See Your Smart Devices? — Privacy From Landlords and Roommates

Privacy from landlords, roommates, and whoever set it up

Tech Made Simple. Service Made Personal.

Bill Davis — Bill's Home Tech

(330) 200-8042 · bill@billshometech.com · Atwater, Ohio

Book a visit · billshometech.com/book

What's Inside

Everything in this guide, with page numbers. Skip to whichever chapter answers your question right now.

The 60-Second Version 3

The Key Principle: It's the Account 4

Renting — What About Your Landlord? 6

Roommates and Family — Shared Access 9

Previous Owners, and How to Take Control 12

Plain Questions and Answers 14

Own the Accounts, Own the Privacy 15

Everyday Cheat Sheet 18

A Picture to Follow Along 19

A Second Look 20

A Note From Bill 20

Your Visit — and My Promise 21

THE 60-SECOND VERSION

1 The 60-Second Version

The whole thing in a breath.

Smart-home devices — cameras, video doorbells, smart locks, thermostats, speakers — are convenient, but they raise a real privacy question when you share or rent a home: who else can see or control them? The key to the whole thing is one simple principle: whoever controls the account a smart device is linked to controls the device.

Smart devices are tied to an online account (set up when the device was installed), and whoever owns and can log into that account can see what the device sees (a camera's feed), control it (the locks, the thermostat), and change its settings — so privacy comes down to who has access to those accounts.

That principle explains the specific worries. Landlords: if a rental came with smart devices that are on the landlord's account, the landlord may still be able to see those cameras or control those locks — a genuine privacy and, often, legal concern. Roommates or family: anyone who shares access to a device's account (or has it set up on their phone) shares the ability to see and control it, so 'shared' smart devices mean shared visibility.

Previous owners: if you moved into a home with smart devices left installed and still linked to the previous owner's account, that person could conceivably still have access until the devices are reset and re-registered to you. The protection in every case is the same: find out whose account each smart device is on, and make sure it's yours — which usually means factory-resetting devices you inherited and registering them fresh to your own account, removing anyone else's access, and being cautious about devices on an account you don't control (like a landlord's).

If you rent, know which devices are yours versus the landlord's, and don't assume a camera isn't being watched just because you live there. Own the accounts, remove others' access, and reset anything inherited — and you control who can see into your home.

- Smart devices (cameras, locks, thermostats, speakers) raise a privacy question when you share or rent: who else can see or control them? The key principle: whoever controls the account a device is linked to controls the device — can see its camera, work its locks, change its settings.
- So privacy comes down to account access. Landlords: a rental's smart devices on the landlord's account may still be seen/controlled by the landlord (a privacy and often legal concern). Roommates/family: shared account access means shared visibility and control. Previous owners: devices left set up and still linked to their account could keep their access until reset and re-registered to you.
- The protection is the same everywhere: find out whose account each device is on, and make it yours.
- That usually means factory-resetting inherited devices and registering them fresh to your own account, removing anyone else's access, and being cautious about devices on an account you don't control (a landlord's). Own the accounts, remove others' access, reset anything inherited — and you control who can see into your home.

THE PRINCIPLE

2 The Key Principle: It's the Account

Whoever controls it, controls the device.

The single idea that explains all of smart-device privacy is this: a smart device is controlled by whoever controls the online account it's linked to. Grasp that, and every question about who can see or control your devices becomes a question about who has access to the account.

- Smart devices link to an online account: when a smart device is set up, it's registered to an online account (in the maker's app), and that account is the key to the device — it's how the device is controlled and viewed.
- Whoever controls the account controls the device: whoever owns and can log into that account can see what the device sees (a camera's video), control it (lock/unlock a lock, set a thermostat, use a speaker), and change its settings — full control.

- It's not about who's physically there: crucially, this account access doesn't depend on being in the home — someone with the account can see and control the device remotely from anywhere, which is exactly why it's a privacy concern.
- So the question is always: whose account?: every privacy question about a smart device reduces to this — whose account is the device linked to, and who can log into it? That's who can see and control it.
- Shared access shares control: if more than one person has access to the account (or the device added to their app), they all share the ability to see and control it — access can be shared with others.
- This is the lens for everything: landlords, roommates, and previous owners are all just specific cases of the same question — who has access to the account the device is on — which the next chapters apply.

The single idea that unlocks all of smart-device privacy, and that everything else in this guide follows from, is this: a smart device is controlled by whoever controls the online account it's linked to. When any smart device is set up — a camera, a video doorbell, a smart lock, a thermostat, a speaker — it's registered to an online account, typically within the device maker's app, and that account is effectively the key to the device, because the account is how the device is controlled and viewed.

This means that whoever owns and can log into that account holds full power over the device: they can see what the device sees (for a camera, that's its live video and recordings), they can control it (locking or unlocking a smart lock, adjusting a thermostat, using or listening through a speaker), and they can change its settings.

The crucial and often-unsettling part is that this account access does not depend on being physically present in the home — someone who has the account can see and control the device remotely, from anywhere in the world, through the app on their own phone, which is precisely why it's a genuine privacy concern rather than a theoretical one: a person with the account doesn't need to be in your house to watch your camera or operate your locks.

Because of all this, every privacy question you might have about a smart device reduces to one and the same question: whose account is this device linked to, and who can log into that account? Whoever that is can see and control the device, full stop. And it follows that if access to the account is shared among more than one

person — whether because several people know the login, or because the device has been added to more than one person's app — then all those people share the ability to see and control the device, since account access can be and often is shared with others.

This one principle is the lens through which to understand every specific situation: the worries about landlords, roommates, and previous owners that the following chapters address are all simply particular cases of the same underlying question — who has access to the account the device is on — so once you hold the principle firmly, you can reason about any smart-device privacy question for yourself.

Whoever controls the account controls the device: that's the whole foundation.

> **GOOD TO KNOW**
>
> The key to all smart-device privacy: a smart device is controlled by whoever controls the online account it's linked to (set up in the maker's app). That person can see what the device sees (a camera's video), control it (locks, thermostat, speaker), and change its settings — and crucially, remotely, without being in the home. So every privacy question reduces to: whose account is the device on, and who can log in? Shared account access means shared control. Landlords, roommates, and previous owners are all just cases of this one question.

LANDLORDS

3 Renting — What About Your Landlord?

Devices on their account are theirs to see.

For renters, the pressing worry is the landlord: if your rental came with smart devices, could the landlord be watching a camera or controlling the locks? The answer follows the account principle — and it's a genuine concern worth taking seriously. Here's how to think about it.

- Landlord-provided devices may be on their account: if your rental came with smart devices already installed by the landlord, those devices may well be linked to the

landlord's account — which, by the principle, means the landlord could see and control them.

- That means possible watching or control: a landlord with the account for a camera could potentially view its feed, and one with the account for a smart lock could potentially see lock activity or control it — a real privacy concern inside your home.
- It's often a legal/ethical concern too: a landlord monitoring inside a tenant's home via cameras raises serious privacy and often legal issues (laws vary by place) — so it's not just uncomfortable, it may be improper or unlawful.
- Find out which devices are the landlord's: the first step is to know which smart devices in your rental belong to and are controlled by the landlord versus which (if any) are yours — ask, and look at what's installed.
- Don't assume a camera isn't watched: a key caution — don't assume a camera in your rental isn't active or being viewed just because you live there; if it's on the landlord's account, it could be.
- Protect yourself: for devices on the landlord's account you can't control, your options include asking the landlord about them and their access, covering or unplugging cameras in private areas where appropriate, and knowing your rights — and for any devices that are meant to be yours, making sure they're on your account, not the landlord's.

For renters, the most pressing version of this worry is the landlord: if your rental came with smart devices already in place — a video doorbell, cameras, a smart lock, a thermostat — could your landlord be watching a camera inside your home or controlling the locks? The answer follows directly from the account principle, and it is a genuine concern worth taking seriously rather than dismissing.

If the smart devices in your rental were installed by the landlord and are linked to the landlord's account, then by the principle that whoever controls the account controls the device, the landlord could potentially see and control them: a landlord holding the account for a camera could view that camera's feed, and one holding the account for a smart lock could see when it's locked and unlocked or even control it, which is a real and uncomfortable privacy concern when it's the inside of the home you're living in.

Beyond the discomfort, this is very often a legal and ethical matter too: a landlord monitoring the interior of a tenant's home through cameras raises serious privacy

issues and frequently crosses legal lines, with the specifics depending on where you live and the laws there, so it may be not merely intrusive but actually improper or unlawful — which is worth knowing, because it means you may have rights here, not just unease.

The practical first step is simply to find out which smart devices in your rental belong to and are controlled by the landlord, versus which ones (if any) are yours — something you can establish by asking the landlord directly and by looking at what's actually installed and how it's set up. A key caution that follows is not to assume that a camera in your rental is inactive or unwatched simply because you're the one living there: if it's on the landlord's account, it could well be active and viewable by them, so you shouldn't treat its presence as harmless by default.

To protect yourself, your options for devices that are on the landlord's account and that you therefore can't control include asking the landlord plainly about those devices and whether and how they access them, covering or unplugging cameras in genuinely private areas where it's appropriate and permitted to do so, and understanding your rights as a tenant regarding monitoring (which vary by location and may warrant looking up or seeking advice on).

And for any devices that are supposed to be yours — ones you brought or that are meant to be under your control — the essential thing is to make sure they are actually registered to your own account and not to the landlord's, so you, and not they, control them. The bottom line for renters is to apply the account principle clearly: know which devices are on the landlord's account, treat those as potentially visible to the landlord, and take sensible steps to protect your privacy, including knowing that monitoring inside your home may raise real legal issues.

WATCH OUT

If your rental came with smart devices installed by the landlord, they may be on the landlord's account — meaning the landlord could potentially see a camera's feed or control the locks, remotely. A landlord monitoring inside a tenant's home via cameras also often raises serious privacy and legal issues (laws vary). So find out which devices are the landlord's, don't assume a camera isn't being watched just because you live there, make sure any devices meant to be yours are on your account, and know your rights.

Rather not do this yourself? I'll come to your home and set it up for you — a flat $99 first visit across Portage County, Ohio and nearby communities. Outside the area? I also help remotely by phone or screen-share. Book at billshometech.com/book or call (330) 200-8042.

ROOMMATES & FAMILY

4 Roommates and Family — Shared Access

Shared account, shared visibility.

When you share a home with roommates or family, smart-device privacy comes down to who shares access to the devices' accounts: shared access means shared visibility and control, which is fine when everyone's on the same page but a problem when someone has more access than you realized. Here's how it works.

- Shared access means shared control: if a smart device's account is shared among roommates or family (several people can log in, or the device is on multiple people's apps), they all share the ability to see and control it — by the account principle.
- That can be fine, or not: shared control is perfectly fine when everyone agrees and trusts each other (a family all controlling the household thermostat, say) — the concern is when someone has access you didn't realize or didn't intend.
- Know who has access to each device: the key is simply to know who can see and control each shared device — check whose accounts have access, so there are no surprises about who can view a camera or work a lock.

- Cameras are the sensitive case: a shared household camera means everyone with access can see its feed, which may be fine in common areas but is a real concern for any private space — be thoughtful about camera placement and access.
- Removing access when people leave: when a roommate moves out, or a relationship changes, remember to remove their access to shared smart devices (and change shared passwords) — otherwise they may keep the ability to see and control them after they've gone.
- Set up access deliberately: rather than everyone sharing one login loosely, set up access deliberately — giving each person the access they should have and no more — so control over the home's devices matches who should actually have it.

When you share a home with roommates or family members, smart-device privacy comes down to who shares access to the devices' accounts, and the principle applies cleanly: shared account access means shared visibility and control. If a smart device's account is shared among the people in the household — whether because several of them can log into the same account, or because the device has been added to multiple people's apps — then by the account principle they all share the ability to see and control that device.

It's important to say that this shared control is perfectly fine, and indeed the whole point, when everyone involved agrees and trusts one another: a family all being able to control the household thermostat, or everyone being able to see the front-door camera, is sensible and convenient. The concern arises specifically when someone has access that you didn't realize they had or didn't intend them to have, which is where shared access turns from a feature into a privacy problem.

The key, therefore, is simply to know who can see and control each shared device — to check whose accounts have access to each one, so that there are no surprises about who can, for instance, view a camera's feed or operate a lock. Cameras are the most sensitive case by far: a shared household camera means that everyone with access to it can see whatever it sees, which may be entirely appropriate for a common area like a shared living room or a front entrance, but is a real privacy concern for any more private space, so it's worth being thoughtful both about where cameras are placed and about who has access to them.

A particularly important and easily-forgotten point concerns people leaving: when a roommate moves out, or a relationship changes, you should remember to remove their access to shared smart devices and to change any shared passwords, because otherwise that person may retain the ability to see and control those devices — including watching cameras in your home — even after they've physically gone, which is a genuine and sometimes serious privacy risk.

More broadly, the sensible approach to shared living is to set up access deliberately rather than letting everyone share one login loosely: giving each person the access they ought to have and no more, so that control over the home's smart devices matches who should actually have it, and so that it can be cleanly adjusted when the household changes.

Applied to roommates and family, the account principle means being clear and deliberate about who has access to what, keeping cameras especially in mind, and promptly removing access when people leave — which keeps shared smart devices a convenience rather than a privacy hazard.

GOOD TO KNOW

With roommates or family, shared account access means shared visibility and control — fine when everyone agrees and trusts each other, a problem when someone has access you didn't realize or intend. So know who can see and control each shared device. Cameras are the sensitive case — everyone with access sees the feed (fine in common areas, a concern for private spaces). Crucially, when a roommate moves out or a relationship changes, remove their access and change shared passwords, or they may keep control after they've gone. Set up access deliberately.

PREVIOUS OWNERS & FIX

5

Previous Owners, and How to Take Control

Reset inherited devices; own the accounts.

Two final things: the risk from previous owners of devices you inherited, and the overall fix that protects your privacy in every case — making sure you own the accounts. Here's both.

- Inherited devices may still link to a previous owner: if you moved into a home with smart devices left installed, or bought used smart devices, they may still be linked to the previous owner's account — meaning that person could conceivably still see or control them until that's changed.
- The fix — factory reset and re-register: the reliable fix is to factory-reset any inherited smart device (which clears its old setup) and then set it up fresh on your own account, which disconnects the previous owner and makes you the sole controller.
- Do this with any device you didn't set up yourself: as a rule, with any smart device you didn't personally set up — inherited, secondhand, or of unknown history — reset it and register it to your own account so you know no one else has lingering access.
- The overall protection — own the accounts: across every case (landlord, roommates, previous owners), the protection is the same: make sure the smart devices you rely on are on accounts you own and control, with no one else having access you didn't intend.
- Check whose account, and remove others: review your smart devices to see whose account each is on and who has access, remove anyone who shouldn't be there, and use strong, private passwords (and two-factor where offered) so no one else can get into your accounts.
- When unsure, reset it: if you're ever unsure who might have access to a smart device, the safe move is to factory-reset it and set it up fresh on your own account — which guarantees a clean slate under your control.

Two final things round out smart-device privacy: the particular risk from previous owners of devices you've inherited, and the overall fix that protects your privacy in every case. On previous owners: if you moved into a home that came with smart

devices already installed, or if you bought used smart devices, those devices may still be linked to the previous owner's account, which — by the account principle — means that the previous owner could conceivably still see or control them, until that link is changed.

A camera left set up and still tied to a previous occupant's account, for instance, could in principle still be viewable by them, which is clearly not something you want in your new home. The reliable fix for this is to factory-reset any inherited smart device, which wipes its old setup and disconnects it from whatever account it was on, and then to set it up fresh on your own account, which makes you the sole controller and removes the previous owner entirely.

As a general rule, you should do exactly this with any smart device you didn't personally set up — anything inherited with a home, bought secondhand, or of unknown history — resetting it and registering it to your own account so that you can be confident no one else has lingering access to it. That points to the overall protection that applies across every situation in this guide, whether it's a landlord's device, a roommate's access, or a previous owner's leftover link: the protection is always the same in essence, which is to make sure that the smart devices you rely on are on accounts that you own and control, with no one else having access you didn't intend to give.

Concretely, that means reviewing your smart devices to find out whose account each one is on and who has access to it, removing anyone who shouldn't be there, and securing your accounts with strong, private passwords (and two-factor authentication where it's offered) so that no one else can get into them and gain access to your devices.

And whenever you're genuinely unsure who might have access to a particular smart device, the safe and decisive move is simply to factory-reset it and set it up afresh on your own account, which guarantees a clean slate entirely under your control and removes any doubt. Taken together — reset anything you inherited, own the accounts for the devices you rely on, remove others' access, and reset when in doubt — these steps put you firmly in control of who can see into your home through its smart devices, which is the whole goal, turning the account principle from a worry

into the very thing that protects you.

> **TIP**
>
> Protect your privacy in every case by owning the accounts. Factory-reset any smart device you didn't set up yourself (inherited with a home, bought secondhand, or of unknown history) and register it fresh to your own account — this disconnects any previous owner. Review your devices to see whose account each is on and who has access, remove anyone who shouldn't be there, and secure your accounts with strong private passwords and two-factor where offered. When unsure who has access, reset it and set it up fresh — a guaranteed clean slate.

QUESTIONS

6 Plain Questions and Answers

The things people ask most.

"Who can actually see or control my smart devices?"

Whoever controls the online account the device is linked to. A smart device is set up on an account (in the maker's app), and whoever can log into that account can see what the device sees (a camera's feed), control it (locks, thermostat, speaker), and change its settings — and they can do this remotely, without being in your home. So every privacy question comes down to whose account the device is on and who can log in. Shared account access means shared control.

"Can my landlord watch cameras or control locks in my rental?"

Potentially, if those devices are on the landlord's account — whoever controls the account controls the device, remotely. A landlord monitoring inside a tenant's home via cameras also often raises serious privacy and legal issues (laws vary by place). So find out which smart devices in your rental are the landlord's, don't assume a camera isn't being watched just because you live there, make sure any devices meant to be yours are on your own account, and know your rights as a tenant.

"What about roommates or family?"

If a device's account is shared, everyone with access shares the ability to see and control it — fine when everyone agrees and trusts each other, a concern when someone has access you didn't intend. So know who can see and control each shared device, be especially thoughtful about cameras (everyone with access sees the feed), and crucially, when a roommate moves out or a relationship changes, remove their access and change shared passwords, or they may keep control after leaving.

"I moved into a place with smart devices already there — are they safe?"

Not necessarily, until you take control. Inherited or secondhand smart devices may still be linked to the previous owner's account, meaning they could conceivably still see or control them. The fix is to factory-reset any device you didn't set up yourself and register it fresh to your own account, which disconnects the previous owner and makes you the sole controller. As a rule, reset anything inherited, of unknown history, and when in doubt — a clean slate under your control.

WRAP UP

7 Own the Accounts, Own the Privacy

Control who can see into your home.

Smart-home devices are wonderfully convenient, but when you share a home or rent, they raise a real question of who else can see or control them — and the key to the whole thing is one simple principle: whoever controls the account a smart device is linked to controls the device, able to see what it sees, operate it, and change its settings, all remotely.

Every privacy question comes down to whose account the device is on. For renters, that means a landlord whose account holds the rental's cameras or locks could potentially watch or control them — a privacy concern that often raises legal issues too — so you should know which devices are the landlord's, not assume a camera isn't being watched, and keep any devices meant to be yours on your own account.

With roommates or family, shared account access means shared visibility and control, which is fine among people who trust each other but requires knowing who has

access, being careful about cameras, and removing access promptly when someone leaves. With a home or devices inherited from a previous owner, those devices may still link to that person's account, so you reset them and register them fresh to yourself.

And the protection in every case is the same: own the accounts for the devices you rely on, factory-reset anything you didn't set up yourself or whose access you're unsure of, remove anyone else's access, and secure your accounts with strong passwords. Do that, and you take full control of who can see into your home through its smart devices — so the convenience never comes at the cost of being watched or controlled by someone you didn't intend.

Own the accounts, and you own the privacy.

- Smart devices raise a privacy question when you share or rent: who else can see or control them? The key principle: whoever controls the account a device is linked to controls the device — can see its camera, work its locks, change its settings, remotely.
- Landlords: a rental's smart devices on the landlord's account may be watchable/controllable by them (a privacy and often legal concern) — know which devices are theirs, don't assume a camera isn't watched, keep yours on your own account. Roommates/family: shared access means shared control — know who has access, mind cameras, and remove access when people leave.
- Previous owners: inherited or secondhand devices may still link to their account — reset and re-register them to you.
- The protection everywhere: own the accounts for devices you rely on, factory-reset anything you didn't set up yourself or are unsure about, remove others' access, and secure accounts with strong passwords. Own the accounts, own the privacy.

GOOD TO KNOW

If you're wondering who can see or control the smart devices in your home — especially if you rent, share with others, or moved into a place with devices already there — I'm happy to help you take control. The key is that whoever controls a device's account controls the device, so we'd find out whose account each of your cameras, locks, and so on is on. For a rental, that means knowing which devices are the landlord's (and not assuming a camera isn't watched); for shared homes, knowing who has access and removing it when people leave; and for anything inherited, factory-resetting it onto your own account. We'll make sure you own the accounts for what you rely on — so you control who can see into your home.

CHEAT SHEET

Everyday Cheat Sheet

Keep this page handy. It points you straight to what to do for each task.

I want to...	Do this...
the key principle	Whoever controls the account controls the device
landlord-provided devices	If it's on their account, they may have access
roommates/family	Shared access means shared visibility and control
previous owners	Devices left set up may still link to their account
check and reset	See whose account devices are on; reset if unsure
protect your privacy	Own the accounts; remove others' access
Get help	Call Bill: (330) 200-8042

AT A GLANCE

A Picture to Follow Along

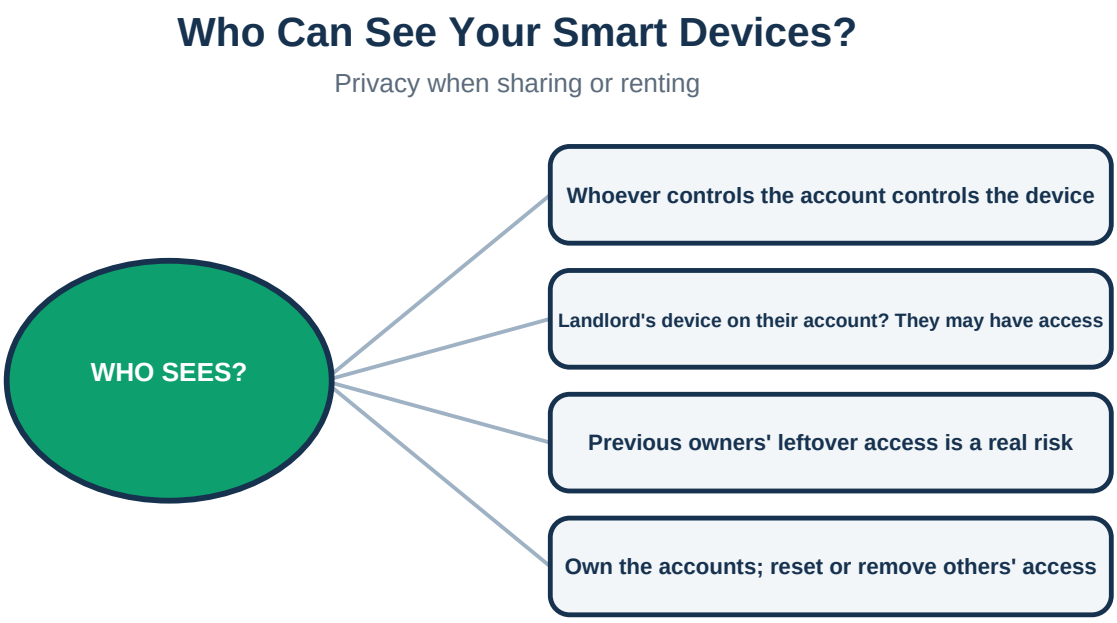


Illustration — a schematic. Set-up screens differ; each takes only a few minutes.

AT A GLANCE

A Second Look

Taking Control

Four steps

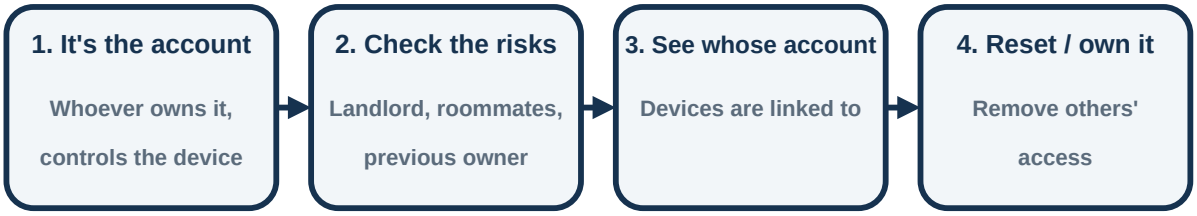


Illustration — a schematic. The order is a suggestion; do one box at a time.

A schematic of the plan — company steps vary; the order does not have to.

BEFORE YOU GO

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 results.

HOW I CAN HELP

Your Visit — and My Promise

You don't have to remember all of it — just that a friendly, patient person is one call away, whenever you'd rather have a hand.

KEY SPECS

In your home — $99 flat for the first visit, no contracts and no surprises, with a 30-day come-back-free follow-up. In-home visits cover Portage County, Ohio and nearby communities.
Outside the area? Remotely — $49 for a screen-share session (free for Support Plan members, $39/mo), refundable if I can't fix it — and credited toward a visit if you'd rather have me in person. Book either at billshometech.com/book.

GOOD TO KNOW

My promise — If you're not 100% satisfied with your visit, I'll come back at no charge, or refund the full $99. No questions, no awkwardness. That's how I'd want to be treated.

Whenever you're ready, I'll come to your home anywhere in Portage County, Ohio and nearby communities, at your pace. Too far for a house call? I also help remotely. Book at billshometech.com/book or call (330) 200-8042. — Bill

Call or text (330) 200-8042 · bill@billshometech.com

This free guide is for general information only — not professional advice, and no substitute for your device's own manual. Any prices or outside products mentioned can change; please confirm current details before you buy. Please use your own good judgment and follow it at your own risk — for anything involving electricity, gas, water, or heights, stop and call a licensed professional. Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results. © 2026 Bill's Home Tech, LLC.