



An Extended Guide · No. 1851

# Keeping Cameras on Their Own Network — A Simple Separation Plan

---

Wall the cameras off from the register, office, and guest Wi-Fi

**Tech Made Simple — Service Made Personal**

[BillsHomeTech.com](http://BillsHomeTech.com) · (330) 200-8042 · Atwater, Ohio

Free & printable — share it with someone who needs it



Book a visit —  
[billshometech.com/book](http://billshometech.com/book)

**! Read this first — it's about people, not just pictures**

Before the gear, a word that matters more than any camera: with a business you are recording other people — customers, staff, people walking by — so where you point a camera, and whether it picks up sound, is as important as the picture. As a rule, keep cameras on general work and public areas, never on restrooms, changing areas, or anywhere someone expects privacy, and be very careful about recording audio. This guide gives you plain-English general information, not legal advice. For your own situation — especially anything to do with employees, audio, or the law — check with an attorney who knows Ohio. Keeping cameras on their own network is partly about privacy too — it keeps camera video away from the systems that hold your customers' and staff's personal and payment details.

## Give your cameras their own lane

A camera that gets hacked shouldn't be able to reach your cash register or your customer records. This guide shows you a simple way to keep your cameras in their own lane — away from the money, the office computers, and the guest Wi-Fi — so one problem can't become a disaster.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. In 30-plus years of helping folks with technology, I've learned that the quiet, boring protections are often the ones that save the day. Keeping cameras separate from the rest of your business is exactly that kind of protection.

It sounds technical, but the idea is plain common sense: don't let the security cameras share a hallway with the safe. We'll keep the jargon to a minimum and focus on what it does for you and how to get it done.

**★ Not sure how yours is wired up?**

If you've got cameras and a register sharing one network and you're not sure whether that's a problem, call or text me at (330) 200-8042. I can look at how it's set up and tell you plainly — free, with nothing to sell you.

## The whole guide, on one page

If you remember only these things, your cameras won't become a back door into the rest of your business.

- ❑ Put your cameras and recorder on a SEPARATE network from your point-of-sale, office PCs, and guest Wi-Fi.
- ❑ That way, if a camera is ever hacked, it can't reach your payment systems or business data.
- ❑ A VLAN — a software-divided network — does this on the gear you already have, without running new wire.
- ❑ Keep guest Wi-Fi separate too, so visitors never touch your business systems or your cameras.
- ❑ Bonus: separating also keeps camera traffic from clogging the office network.

### ✓ One rule to hold onto

Think of each network as a room with a locked door between them. The cameras, the register, the office, and the guests each get their own room — so trouble in one can't wander into the others.

## Why cameras don't belong with the register

Cameras are little computers, and like any computer they can be compromised. The question is what a compromised camera can reach.

If your cameras share one flat network with your point-of-sale, your office computers, and everything else, then a camera that gets hacked is standing in the same room as all of it. From there, an intruder can go looking for your payment systems and your business data — the crown jewels.

Put the cameras on their own network, and that changes completely. Now a hacked camera is in a locked room by itself. It can't see the register, it can't reach the office files, and the problem stays contained to the one place it started. Same cameras, same building — but a world of difference in what can go wrong.

### **! Cameras are a favorite way in**

Cameras get picked on precisely because they're everywhere, often forgotten, and sometimes left on weak passwords. That makes them a favorite foothold for attackers. Keeping them in their own lane means that foothold leads nowhere.

## A VLAN, in plain English

You'll hear the word VLAN a lot in this subject, and it sounds more complicated than it is. Here's the whole idea in one breath.

A VLAN is a **software-divided network**. Instead of running separate wires and buying separate equipment for each group, you use settings on gear you already have to split one physical network into several that can't talk to each other. The cameras live on one, the register on another, the office on a third, the guests on a fourth.

Picture one big office building with a single front door, and then picture walls and locked doors added inside so each department has its own suite. Nobody rewired the building — they just divided it up. A VLAN does the same thing to your network: same wires, but walls where it counts.

You don't have to set this up yourself or even fully understand it. You just need to know it exists, know your cameras should be on their own one, and know to ask for it when the system goes in.

### ✓ The word matters less than the result

Whether someone calls it a VLAN, a separate network, or 'putting the cameras on their own subnet', the goal is the same: the cameras in one locked room, the money and data in another. Ask for the result and let the tech sort out the term.

## Keep the cameras away from payment systems

If there's one thing to wall off from the cameras, it's anything that touches payments. This is where the real damage happens.

Your point-of-sale and card systems handle your customers' payment details, and that makes them the prize an attacker is really after. A camera network that can reach the payment network is a bridge straight to that prize. Cut the bridge — put payments and cameras on separate networks — and a hacked camera simply can't get there.

This isn't only good sense; keeping card systems walled off from everything else is a basic expectation in handling payments. Separating the cameras is one natural piece of that. If you take card payments, talk to whoever set up your payment system about keeping it on its own, too.

### **! The payment network is the one to guard hardest**

A stolen camera feed is bad. Stolen customer payment data is a different order of trouble — for your customers and for you. If you separate just one thing, separate the payment systems from everything else, cameras very much included.

## Keep guest Wi-Fi on its own, too

The Wi-Fi you offer customers is another network that should never touch your business systems — or your cameras.

When you let customers onto your Wi-Fi, you're letting strangers' phones and laptops onto a network. If that guest Wi-Fi shares a lane with your register, your office, or your cameras, you've handed every visitor a starting point inside your business. Keep guest Wi-Fi walled off on its own, with no path to anything that matters.

Most business-grade equipment makes this easy — a separate guest network is a common, built-in feature. The key is making sure it's truly separate, not just a second name on the same network. Guests should be able to reach the internet and nothing else of yours.

- Guest Wi-Fi reaches the internet only — never your register, office, or cameras.
- Give it its own name and password, changed now and then.
- Don't run your own business devices on the guest network for convenience.
- If you don't need to offer guest Wi-Fi at all, that's one fewer door to guard.

### ✓ Four lanes, not one

A tidy small business often has four lanes: payments, office, cameras, and guests — each walled off from the others. It sounds like a lot, but it's usually settings on one good piece of equipment, not four separate systems.

## A bonus: no more clogged office network

Separation isn't only about security. It also keeps your cameras from bogging down everything else.

Video is heavy. A building full of cameras streaming to a recorder moves a lot of data around your network all day long. If that camera traffic shares a lane with your office computers and your point-of-sale, it can slow them down — a card reader that hesitates, a file that crawls — at the worst possible moment.

Put the cameras on their own network and that heavy video traffic stays in its own lane, where it belongs. The office runs smoother, the register responds quicker, and the cameras get the room they need. One change, two payoffs — safer and faster both.

### ✓ **Faster and safer, same move**

Owners who separate their cameras for security often tell me the surprise benefit was the office finally feeling snappy again. The same wall that keeps the cameras contained keeps their traffic out of your way.

## What it takes to set this up

You don't need a server room. For most small businesses, separation comes down to the right equipment and the right settings.

The ability to split your network into lanes lives in business-grade network equipment — the kind that supports VLANs and guest networks. Plenty of small businesses already have gear that can do it and just haven't had it set up. Some older or very basic home-style equipment can't, and that's worth knowing before you count on it.

Setting it up is a settings job, not a wiring job — which lane each camera and device belongs to, and which lanes are allowed to talk. It's fiddly to get exactly right, but it's a one-time setup. Once the walls are built, adding a camera to the right lane is quick.

### ★ I'll tell you what your gear can do

Not sure whether your network equipment can keep the cameras separate? Tell me what you've got, or send a photo of it, and I'll tell you whether it can do the job or whether a better piece would earn its keep. Call (330) 200-8042.

## You can still watch from your phone

A common worry: if the cameras are walled off, can I still see them from my phone? Yes — and safely.

Separating the cameras doesn't cut off your remote viewing. The maker's secure app reaches the cameras through the maker's own service, and a VPN tunnels you safely onto the camera network when you need it. Neither of those requires tearing down the walls between your networks.

What separation does rule out is the dangerous shortcut — opening a port on the router so the recorder sits on the open internet. That was never safe anyway, and our remote-viewing guide covers the safe paths in detail. Separation and safe viewing go hand in hand.

### ✓ Walls inside, safe door out

Think of it as walls between your internal networks, plus one safe, locked door to the outside for your phone — the maker's app or a VPN. You get the protection and the convenience both.

## Two kinds of businesses, two sets of needs

A busy storefront and a quieter office or warehouse both benefit from keeping cameras separate — but the networks they're protecting look a little different.

### If you run a customer-facing shop or storefront

You've got payment systems handling customer cards, maybe guest Wi-Fi, and cameras all over the floor. That's exactly the mix where separation pays off most.

- Wall the cameras off from your point-of-sale above all else.
- Keep guest Wi-Fi on its own lane, reaching the internet only.
- Keep heavy camera video off the lane your card readers use.
- Give the office computers their own lane, separate from both.

### If you run an office, warehouse, or back-of-house

Fewer card payments, perhaps, but sensitive business data, expensive stock records, and lots of cameras over big spaces. The data is what you're guarding.

- Wall the cameras off from the computers holding your business data.
- Keep the heavy traffic from many cameras in its own lane.
- If you have any payment or ordering systems, separate those too.
- Plan the lanes once, up front, so adding cameras later is easy.

#### ★ Let's map your lanes

Tell me what systems you run — register, office, cameras, guest Wi-Fi — and I'll help you sketch which lanes you need and how to keep them walled off. Call (330) 200-8042.

## Getting the separation actually right

A wall with a gap in it isn't a wall. The value is all in doing the separation properly, so there's no quiet path around it.

The common mistake is thinking you're separated when you're not — a camera accidentally left on the office lane, a guest network that can still reach the register, a rule that allows more than it should. The walls only protect you if there are no doors you forgot to lock.

That's why this is worth getting checked rather than assumed. After it's set up, the right person can confirm that each lane really can't reach the others — that a device on the camera network genuinely can't see the payment network, and a guest phone genuinely can't see either. Trust, then verify.

### **! Assumed separation is no separation**

I've seen plenty of networks that everyone believed were separated but weren't — one stray setting left a door wide open. Don't take it on faith; have someone confirm the walls actually hold before you rely on them.

## Separation plus strong passwords

A separate network buys you time and containment. Strong passwords keep the camera from being hacked in the first place. You want both.

Think of separation as the second line of defense. The first line is not letting the camera get compromised at all — strong, unique passwords on every camera and the recorder, the default admin accounts disabled, and firmware kept current. Our passwords-and-updates guide walks through all of it.

With both in place, you're covered two ways: the strong passwords make a camera hard to take over, and the separate network means that even if one somehow is taken over, it leads nowhere. Belt and suspenders — which is just how you want your payment data protected.

### ✓ Don't rely on the wall alone

Separation is powerful, but it's not a reason to get lazy about passwords. A hacked camera on its own network still means someone's watching your feed. Lock the camera down and wall it off — both.

## Separation and keeping data private

Keeping networks separate isn't only a technical nicety — it's part of protecting the people whose information you hold.

Your business holds things people trust you with: customers' payment details, employees' records, maybe more. Keeping the cameras — and guests, and anything exposed — walled off from the systems that store that information is part of being a careful custodian of it. A breach that spreads from a camera to customer data is exactly the kind of harm separation prevents.

The cameras themselves still follow all the usual rules — general work and public areas only, never private spaces, and care with audio — no matter which network they're on. We cover those in their own guides.

### **! A quick word on handling data**

If you store customer payment or personal information, you may have specific obligations to protect it, and keeping card systems walled off is a basic part of that. This is general information, not legal or compliance advice. This is general information, not legal advice; rules change and every situation is different, so confirm the specifics with an attorney who knows Ohio before you rely on it.

## A simple separation checklist

Run down this list to see whether your cameras are truly in their own lane — or just sharing the hallway with the safe.

- ☐ Cameras and recorder are on their own network, separate from everything else.
- ☐ Payment and point-of-sale systems are on their own lane.
- ☐ Office computers are separate from the cameras.
- ☐ Guest Wi-Fi reaches the internet only — not the register, office, or cameras.
- ☐ Someone has confirmed the lanes really can't reach each other.
- ☐ Remote viewing is through the maker's app or a VPN — no open ports.
- ☐ Every camera and the recorder still have strong, unique passwords.
- ☐ Adding a new camera puts it on the camera lane by default.

### ★ Want me to check the boxes with you?

Separation is easy to get almost right and still leave a gap. I'm glad to walk this checklist with you and confirm each line actually holds. Call or text (330) 200-8042.

## Common mistakes with camera networks

A handful of slip-ups account for most 'separated' networks that aren't really separated. Here they are.

- **One flat network** with cameras, register, office, and guests all sharing a lane.
- **Assuming separation** that was never actually set up or confirmed.
- **Guest Wi-Fi that isn't walled off**, so visitors can reach business systems.
- **A stray camera** left on the office lane when the rest were moved.
- **Relying on the wall alone** and leaving weak passwords on the cameras.
- **Camera traffic clogging** the lane your card readers and computers use.

### ! The gap you didn't know about

Most separation failures aren't dramatic — they're a single device or setting left on the wrong lane, quietly bridging two networks that were supposed to be apart. That's why confirming the walls matters as much as building them.

## What you can do, and when to get help

Understanding the plan is something every owner can do. Building the lanes correctly is where many like a hand.

You can absolutely learn the idea, decide which lanes your business needs, and make sure separation is on your shopping list when you buy equipment or hire an installer. That understanding is half the battle — it's why 'separated networks' gets asked for instead of forgotten.

The actual setup — configuring VLANs, writing the rules about which lane can reach which, and confirming the walls hold — is fiddly, and a small mistake can leave a gap you'd never notice. This is a good place to have someone who does it regularly, whether that's me working with your network gear or a networking pro for a bigger setup.

### ★ I'll set up the lanes and check them

Sorting cameras onto their own network and confirming they can't reach your register is squarely what I do — no wiring, just the setup done right. \$99 for a visit, \$49 on your screen where I can, 30 days come-back-free. Call (330) 200-8042.

## How separation fits the rest of your security

Keeping cameras separate is one layer of three that work together. Each covers what the others can't.

This guide walls the cameras off, so a problem can't spread to your money or data. The remote-viewing guide keeps the connection to your phone safe, so strangers can't reach the cameras from outside. And the passwords-and-updates guide keeps the cameras themselves hard to take over in the first place.

Read together, they answer the three questions that decide whether a camera system is a tool or a liability: where can the cameras reach, who can reach the cameras, and how hard are they to break into. Lean on all three rather than repeating each other's depth here.

### ✓ Three layers, one peace of mind

Separate the networks, view safely, and lock the cameras down with strong passwords and updates. Any one alone helps; all three together is how you stop worrying about your cameras being used against you.

## Plan the lanes before you install

Separation is far easier to build in from the start than to retrofit later. A little planning now saves a redo.

When you're planning a camera system — which our planning guide walks through — decide early that the cameras will live on their own network. That one decision shapes the equipment you choose and spares you untangling a flat network after everything's already running on it.

If you're inheriting or extending an older setup where everything shares a lane, separation may mean sorting out what's there first — our guide on taking over an old system helps with that. Either way, the lanes are worth planning before the cameras go up, not after.

### ★ Build it in from the start

Planning a new system or reworking an old one? Let's make separate lanes part of the plan from day one — it's so much easier than pulling the cameras out of a tangled network later. Call (330) 200-8042.

## Common Questions

The questions I hear most from owners wondering whether their cameras are safely separated.

### **Q: Why should cameras be on their own network?**

So a hacked camera can't reach your payment systems, office computers, or business data. On a separate network, a compromised camera is stuck in a locked room by itself — the problem can't spread to anything that matters.

### **Q: What is a VLAN, exactly?**

A VLAN is a software-divided network. Using settings on gear you already have, it splits one physical network into several that can't talk to each other — like adding locked interior doors to a building without running new wire.

### **Q: Do I need to buy new equipment?**

Maybe not. Many small businesses already have network gear that supports separate lanes and just haven't had it set up. Some older or very basic equipment can't, so it's worth checking what yours can do before you count on it.

### **Q: If I separate the cameras, can I still watch from my phone?**

Yes. The maker's secure app and a VPN both reach the cameras without tearing down the walls. The only thing separation rules out is the dangerous open-port shortcut — which you shouldn't use anyway.

#### **★ Still weighing it up?**

Keeping cameras in their own lane is one of the highest-value, lowest-glamour things a business can do. Call or text me at (330) 200-8042 and I'll help you figure out the simplest way to get there.

## Why this quiet step matters so much

Of all the security steps in this series, separation is the one that limits the damage when something slips through. That makes it worth the trouble.

No security is perfect. A password leaks, a device slips through, a mistake happens — it's a matter of when, not if, over enough years. What separation gives you is a world where those slips stay small. A hacked camera is a nuisance. A hacked camera that reaches your customers' payment data is a catastrophe. Separation is the wall between those two outcomes.

That's why I nudge every business owner toward it, even when it sounds like technical over-caution. It's the difference between a bad day and a bad year — and it costs a one-time setup, not a fortune.

### ✓ **Contain the damage you can't prevent**

You can't stop every problem, but you can decide how far one is allowed to spread. Separation is you drawing that line in advance — and it's the best insurance a camera network can have.

## Keeping the walls up over time

Networks drift as businesses change. A quick check now and then keeps your lanes from quietly merging back together.

Every time you add a camera, swap a piece of equipment, or bring on a new device, there's a chance it lands on the wrong lane or a rule gets loosened. Make a habit of confirming, when anything changes, that the new thing went where it belongs and the walls still hold.

Fold this into the same recurring checkup as your passwords and updates — a once-or-twice-a-year look at the whole system. It's a few minutes that keep a carefully separated network from slowly turning back into a flat one.

### ★ Make it a standing visit

I'm glad to make confirming your network separation part of a regular checkup, so you never have to wonder whether a change opened a gap. Call (330) 200-8042 and we'll set up a rhythm that fits your business.

## 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 keeping your cameras on their own network 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 — that's what the guide is for.

When you'd rather have a hand, that's exactly what I do. I come to your place of 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 licensed electrician or low-voltage contractor — for in-wall wiring or panel work I'll help you line up a trustworthy local pro and make sure it all works together.

### ★ 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

## Four Lanes, Walled Off From Each Other

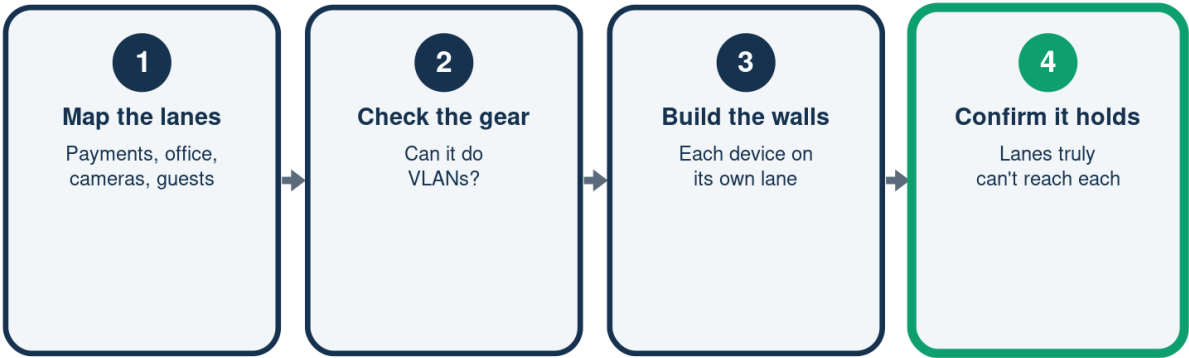
Each network in its own locked room

|          | What it holds  | Who's on it       |
|----------|----------------|-------------------|
| Payments | Card data      | Register only     |
| Office   | Business files | Staff PCs         |
| Cameras  | Video          | Cameras, recorder |
| Guests   | Internet only  | Visitors          |

A problem in one lane can't reach the others.

# Separating Your Cameras in Four Steps

The calm way to wall them off



Do these and a hacked camera leads nowhere.

## Shared Lane vs. Separate Lane

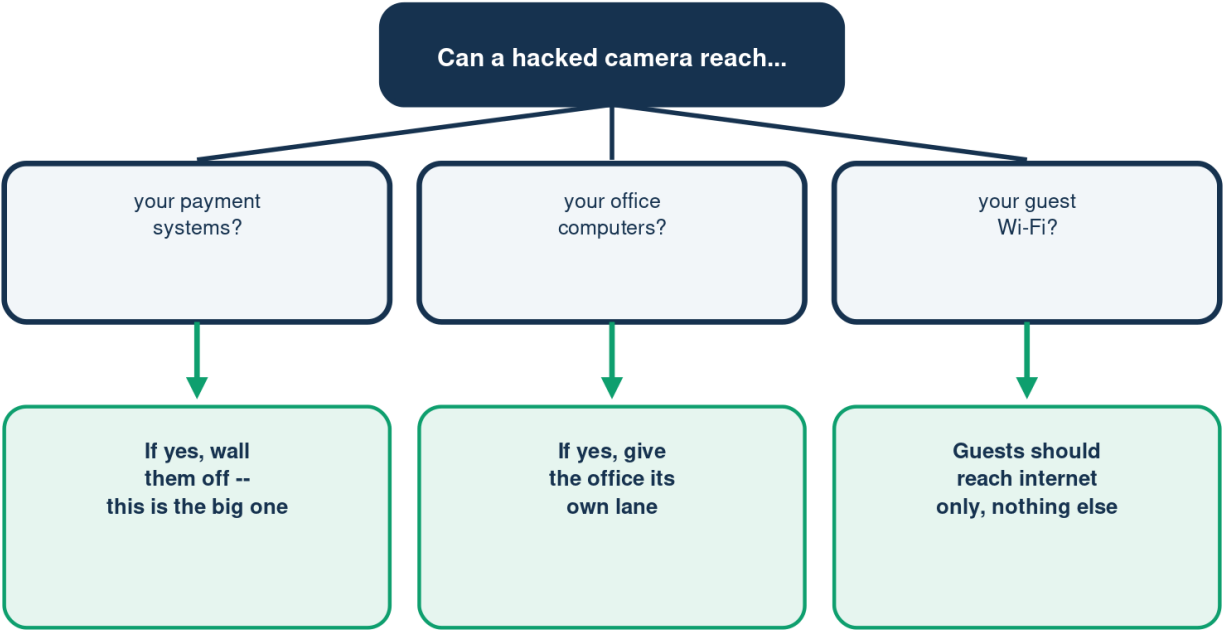
What a hacked camera can reach, each way

|              | One flat network | Separate network |
|--------------|------------------|------------------|
| Payments     | Reachable        | Walled off       |
| Office data  | Reachable        | Walled off       |
| Guest Wi-Fi  | Mixed in         | On its own       |
| Office speed | Clogged          | Snappy           |

Same cameras -- a world of difference in the damage.

# Are My Cameras Really Separated?

Three quick questions to tell for sure



Confirm the walls hold -- assumed separation is no separation.

Illustration - a schematic, not to scale. Your setup may differ.



## Need a Real Person?

You do not have to figure this out alone.

You just have to remember you can call.

Friendly, plain-English 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](https://billshometech.com/book)

Use of these guides is subject to our Terms of Use ([billshometech.com/terms-of-use](https://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