



An Extended Guide · No. 2086

Can You Actually Restore? A Quarterly Backup Fire Drill

Test a file, a mailbox, and a
whole machine — before you need to

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. A backup is half of that safety net — but only the half you've actually tested, because a backup you've never restored may not work when the bad day comes.

Can you actually get your data back?

Most small businesses have a backup of some kind running somewhere. Far fewer have ever tried to restore from it. That gap is where disasters live: the backup that was quietly failing for months, the one missing the files you most needed, the one you couldn't figure out how to use under pressure. This guide turns 'we have backups' into 'we know they work.'

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. The good news is that proving your backup works is simpler than setting one up — it's a short drill you run a few times a year.

Here's the whole idea: a backup isn't real until you've **restored** from it. So four times a year, you run a fire drill — restore a single file, restore an email, and restore a whole machine to a test — and write down that it worked. That's it. Do that, and you never have to wonder whether your safety net is actually there.

★ I'll run your first fire drill with you

If you've never tested a restore, let's do the first one together — I'll show you how to pull back a file, an email, and a whole machine, and leave you with a simple checklist to repeat. Call or text me at (330) 200-8042.

The quarterly fire drill, on one page

If you remember only one thing from this guide, make it this checklist — run it every three months.

- ❑ **Restore a single file.** Pick a document, delete your working copy (or rename it), and bring it back from the backup.
- ❑ **Restore an email or mailbox item.** Recover a specific message or folder to prove your email is really backed up.
- ❑ **Restore a whole machine.** Bring a full computer back to spare hardware or a test setup — not just loose files.
- ❑ **Check the contents.** Open what you restored and confirm it's complete and current, not empty or months old.
- ❑ **Log the date and result.** Write down when you tested and that it worked — this also answers insurance questions honestly.
- ❑ **Confirm one copy is offline or locked away** where ransomware can't reach it.

! An untested backup is a guess, not a safety net

The worst time to discover your backup is broken, incomplete, or impossible to use is the morning after a disaster. The fire drill moves that discovery to a calm Tuesday when you can fix it. Test before you need it — every time.

Why 'we have a backup' isn't enough

It feels like having a backup is the finish line. It's really just the starting line.

Backups fail quietly in a dozen ways. The backup job stops running after an update and nobody notices. It's been copying the wrong folder all along. It saves your files but not your email. It fills up and silently stops. The drive it lives on dies. Each of these looks fine from the outside — the little backup icon is green — right up until the day you actually need to restore and find out it was hollow.

The only way to know a backup works is to use it before you have to. A restore test turns a hopeful assumption into a proven fact. It's the difference between 'I think we're covered' and 'I watched it come back last month.' That certainty is the entire point of this guide — and it's why the drill matters more than which backup product you chose.

! A backup you've never restored may not work

This is the hard lesson behind countless small-business disasters: the backup existed, but it had been failing for months, or didn't contain what they needed, or nobody knew how to bring it back. Having a backup and having a working backup are two different things. Testing is what connects them.

The 3-2-1 idea, in plain English

There's a simple rule of thumb for backups that's worth knowing, and it fits on a napkin.

The **3-2-1** idea says: keep **3** copies of your important data (the working copy plus two backups), on **2** different kinds of storage (so one failure doesn't take both), with at least **1** copy kept offsite or offline (so a fire, theft, or ransomware at your office can't destroy everything at once). It's not fancy, and you don't need special gear to follow it.

In a small office, this often looks like your files on the computer (copy one), a backup to a local drive or network box (copy two, a different kind of storage), and a backup to the cloud or a drive you keep offsite (copy three, offsite/offline). The exact mix matters less than the principle: don't let one bad event reach every copy you have.

✓ The '1' is the one that saves you in a disaster

The offsite-or-offline copy is the hero of the rule. A flood, a theft, or ransomware can wipe out everything plugged into your network at once — but it can't touch the copy that's somewhere else or disconnected. If you get only one part of 3-2-1 right, make it that one.

Why ransomware goes after your backups

Your backup is your get-out-of-ransomware-free card — which is exactly why attackers try to destroy it first.

Ransomware locks up your files and demands payment to unlock them. A good, working backup is how you say 'no thanks' and restore instead of pay. Attackers know this, so modern ransomware deliberately hunts for your backups and encrypts or deletes them too — especially any backup that's connected to the network or always plugged in, where it can reach them the same way it reached your files.

That's the whole case for keeping at least one copy **offline** or **immutable** — a backup the ransomware simply cannot touch because it's disconnected, or because it's set up so that even an attacker can't alter or delete it for a set time. When your office gets hit, that untouchable copy is the one that lets you recover. Our ransomware guide covers the rest of the response; the untouchable backup is the foundation it rests on.

! Keep one copy ransomware can't reach

A backup that's always connected to your network is a backup ransomware can destroy. An offline copy (disconnected) or an immutable one (can't be changed or deleted for a set time) is the one that survives an attack. Make sure at least one of your copies is in that category.

Drill part one: restore a single file

The simplest test, and the one you'll use most in real life — someone deletes or corrupts a file and needs it back.

Pick a real document — not a test file you just made, but something that's genuinely part of your work. Rename your working copy or move it aside, then go to your backup and restore that file. Watch where it lands, open it, and confirm it's the right version with all its contents. Then put things back the way they were.

This sounds trivial, and when it works it is. But it's surprisingly common to discover that the folder you assumed was backed up isn't, or that the restored file is weeks older than you expected, or that you honestly don't know how to find and restore a file in your backup tool. Far better to learn all that now than during a crisis.

✓ Time yourself — how long to get one file back?

Note roughly how long the single-file restore took and how easy it was to find. In a real pinch — an employee deleted the wrong thing an hour before a deadline — knowing you can pull it back in two minutes is its own kind of calm.

Drill part two: restore an email or mailbox

Email is often a business's most important record, and it's the backup people most often assume is handled when it isn't.

Try to recover a specific email, a folder, or a mailbox item from your backup. How you do this depends on your setup — some email systems have their own recovery for recently-deleted items, while a full mailbox backup may live in a separate tool. The test is the same either way: can you get a specific message back, and do you know how?

A very common surprise here is discovering that your email isn't really backed up at all — that you've been relying on the email provider's own limited recovery window, which may only cover recently-deleted items for a short time. If that's the case, this drill just caught a real gap worth closing, because years of business correspondence is hard to replace.

! Don't assume your email provider is your backup

A cloud email service keeps your mail running, but its built-in recovery is often limited and short — it is not the same as a true backup you control. If a full mailbox were lost or an account compromised, could you get it all back? If you're not sure, that's the gap to close.

A few laptops, or a server everyone depends on

The fire drill is the same idea for everyone, but what 'restore a whole machine' means — and how much is riding on it — depends on your setup.

If your data lives on a few laptops and the cloud

With a small shop where everyone works off their own laptop and shared cloud folders, the drill is quick and personal. You're mostly proving you can get files and email back and rebuild a laptop if one dies.

- Restore a file and an email from your cloud and backup tools.
- Prove you could set up a replacement laptop and get someone working again from backup.
- Make sure the cloud's own trash/recovery isn't the only thing standing between you and lost files.
- Keep one backup copy offline or in a separate account ransomware can't reach.

If you run a server or shared system everyone needs

When a server or shared system holds the data your whole team depends on, a failed restore there stops the business. The whole-machine test matters most here, and it's worth doing on spare hardware or a test setup so you know how long a real recovery would actually take.

- Test restoring the full server or system image, not just the files on it.
- Time the restore — how many hours until everyone could work again? That number is your real exposure.
- Keep an offline or immutable copy specifically to survive a ransomware hit on the server.
- Write down the steps so someone other than one person could do the restore in an emergency.

★ Not sure how to test a whole-machine restore?

The whole-machine part trips up a lot of offices, and it's the one that matters most. I can walk you through restoring to a test, time how long it takes, and leave you with a written recovery plan. Call (330) 200-8042.

Drill part three: restore a whole machine

This is the big one — and the one almost nobody tests until it's too late. It's also where the real surprises hide.

Restoring loose files is one thing; bringing back an entire computer — the operating system, the programs, the settings, and all the data — is another. The best way to test it is to restore to **spare hardware** or a **test setup**, so you're not disturbing the machine people are using. The goal is to prove that if a computer died completely today, you could stand up a working replacement from your backup.

Two things to watch for: whether your backup actually captures a full machine (some backups only save files, not the whole system), and how long the restore takes. That time is your real downtime in a disaster. If restoring the server takes two days, that's two days your business is down — much better to know that now and plan for it than to learn it live.

✓ The restore time is a number worth knowing

Write down how long a full restore takes. It tells you your worst-case downtime, it helps you decide whether you need faster recovery, and it's exactly the kind of thing a cyber-insurance application or a recovery plan wants you to know.

Write it down: the restore log

The drill isn't finished until you've logged it. The log is small, and it does a surprising amount of work.

After each quarterly drill, jot down the date, what you restored (file, email, whole machine), whether it worked, how long it took, and anything you fixed. One line per test is plenty. Keep it with your other business records — and not only on a machine that could itself be the thing that fails.

Log this	Why it matters
Date tested	Proves it's current
What you restored	Shows full coverage
Worked? yes/no	Flags problems early
How long it took	Your real downtime
What you fixed	Tracks improvement

✓ **The log answers the insurance question honestly**

Cyber-insurance applications ask whether your backups are tested. A dated restore log lets you answer 'yes' truthfully and prove it — which, as our cyber-insurance application guide explains, is exactly the kind of honest, documented answer that protects your coverage.

What your insurer wants to see

'Tested backups' is a line on nearly every cyber-insurance application — and it's one good businesses accidentally overstate.

Insurers ask whether you keep backups, whether a copy is kept offline or isolated, and whether you've actually tested a restore. They ask because a tested, protected backup is often what lets a business recover from ransomware without a payout. A backup that runs but has never been restored is not a tested backup — and answering 'yes, tested' when you haven't is the kind of overstatement that can come back to bite you after a loss.

The quarterly drill plus a dated log turns this from a stretch into a clean, honest 'yes.' You tested it, you can say when, and you can show the log. As our cyber-insurance application guide puts it, a truthful answer you can prove is worth far more than a hopeful one you can't.

! A quick, important note

This guide explains the idea in plain English so you know what to ask about — it is general information, not legal or insurance advice, and it is not a substitute for reading the actual rule or policy. Laws and requirements change, and your situation may be different, so please confirm the current requirement with a lawyer, your insurance agent, or the agency itself before you rely on it.

Test before you upgrade, too

The quarterly rhythm is the backbone, but a few moments call for an extra, unscheduled test.

Any time you're about to make a big change — upgrading to a new version of Windows, migrating to a new computer, replacing a server — run a quick restore test first. A big upgrade is exactly when things occasionally go sideways, and a confirmed-working backup turns a scary migration into a reversible one. Our updates-and-end-of-support guide covers the upgrades themselves; this is the safety net under them.

The same goes for any time your setup changes in a way that touches backups: a new backup tool, a new storage box, a new cloud service. Don't assume the new thing is capturing everything the old one did — test a restore and confirm. A backup change is the most dangerous moment of all, because everyone assumes it's handled.

✓ A change to the backup itself demands a test

The riskiest backup is the one you just changed and didn't verify. New tool, new drive, new service — run a restore before you trust it. Five minutes of testing beats discovering the new setup was never really working.

Make sure you're backing up the right things

A drill only proves the backup works — not that it covers everything. Step back now and then to check the scope.

It's easy to set up a backup years ago and never revisit what it actually captures. Meanwhile the business changes: new folders, a new accounting program, data that moved to the cloud, a shared drive someone added. A backup faithfully copying last year's setup can miss this year's most important data without a single error message.

- **Your working files and documents** — the obvious core.
- **Email and mailboxes** — often assumed handled when it isn't.
- **Accounting, point-of-sale, and industry software data** — which may live in its own place.
- **Shared drives and network storage** everyone saves to.
- **Cloud data** — your cloud files and email may need their own backup, not just the provider's recovery.

✓ Restore from the user's seat, not the admin's

When you test, pretend you're the person who lost the data. Can you find and restore what a front-desk employee would need? A backup only an expert can navigate is a backup that fails in a real, stressful emergency.

The backup mistakes that bite hardest

Nearly every backup disaster I hear about traces back to one of these. Now you'll know them in advance.

- **Never testing a restore** — trusting a green icon instead of proof.
- **Only one backup copy**, with nothing offsite or offline when disaster strikes.
- **The only backup stays plugged in**, so ransomware encrypts it along with everything else.
- **Backing up files but not the whole machine**, so recovery takes days to rebuild from scratch.
- **Assuming email and cloud data are backed up** by the provider when they're not.
- **No log**, so you can't prove to an insurer — or yourself — that it's ever been tested.

! The green checkmark is not proof

Backup software showing 'last backup successful' tells you a job ran — not that the data is complete, current, and restorable. The only proof is a restore you watched work. Trust the test, not the icon.

Making the quarterly drill actually happen

A test you mean to do and never do protects nobody. The trick is to make it automatic on the calendar, not dependent on remembering.

Pick four dates a year — the first week of each quarter, or tie it to something you already do, like paying quarterly taxes — and put the fire drill on the calendar as a recurring reminder. Give it to a specific person so it's someone's job, not everyone's and therefore no one's. The whole drill takes well under an hour once you've done it a couple of times.

Keep the bar low enough that it actually happens: file, email, machine, log. You're not auditing every byte — you're proving the net still catches. Four short, honest tests a year beat one elaborate test you plan forever and never run.

★ I can set up the reminder and run the first few with you

If a recurring drill sounds like one more thing to forget, I'll set up the schedule, run the first couple with you so it feels easy, and leave you a one-page checklist. After that it's a quick habit. Call (330) 200-8042.

What to do when a test fails

A failed drill isn't bad news — it's the whole point. You just found a disaster before it found you.

If a restore doesn't work — the file is missing, the email won't come back, the whole-machine restore won't complete — resist the urge to feel defeated. You've just turned a future catastrophe into a present, fixable problem, on a day when nothing is actually on fire. That's a win, every time. Note exactly what failed in your log.

Then fix the root cause: maybe the backup wasn't capturing that folder, maybe it had silently stopped running, maybe the storage filled up, maybe nobody knew the restore steps. Fix it, then run the test again to confirm the fix worked. A backup problem you found and fixed on a Tuesday is infinitely better than one you discover the morning after ransomware.

! A failed drill today prevents a failed recovery later

Every backup that failed a real recovery once looked fine — because nobody had tested it. Finding the failure during a drill is the system working exactly as intended. Fix it, retest, and move on with real confidence.

More than one person should know how

A recovery plan that lives in one person's head fails the day that person is on vacation — or has left.

If only one person knows how to restore your backups, you have a hidden single point of failure. Disasters don't wait for the right person to be in the office. Write the restore steps down in plain language — where the backups live, how to reach them, the steps to restore a file and a whole machine — and keep that document somewhere findable, not only on the computer that might be down.

This ties into the bigger picture of not handing anyone the only copy of the keys to your business. The owner should always be able to reach the backups and understand, at least in outline, how recovery works — even if day-to-day it's someone else's job or mine.

✓ Write the recovery steps where a stressed person can follow them

In a real emergency, people don't think clearly. A calm, numbered page — 'here's where the backup is, here's how to restore' — that anyone can follow is worth more than an expert who happens to be unreachable that day.

Where backups fit in the whole picture

A tested backup is the layer that lets you recover from almost anything else that goes wrong.

Picture the layers: two-step sign-in keeps people out of your accounts; updates close the holes attackers use; antivirus catches bad software; encryption protects lost laptops. Backups are different from all of them — they don't prevent trouble, they let you recover from it. When another layer fails, a tested backup is what turns a catastrophe into an inconvenience.

That's why it may be the most important layer of all, and why testing it matters so much. A prevention layer that fails is a bad day; a recovery layer that fails when you finally need it is the end of the road. The quarterly fire drill is how you make sure the layer you're counting on to save you will actually be there.

✓ Backups don't prevent disasters — they end them

Everything else on your security list tries to stop bad things from happening. The backup is the one layer that assumes something bad already did, and gets you back on your feet anyway. Keep it tested, and almost nothing can truly take you down.

Once a year, look a little deeper

The quarterly drill keeps the net working. An annual look makes sure the net is still the right size.

- ❑ Review what you're backing up and whether the business has added new data the backup is missing.
- ❑ Confirm you still have the full 3-2-1 spread, including an offline or immutable copy.
- ❑ Re-check your worst-case restore time and decide if it's still acceptable as you've grown.
- ❑ Make sure more than one person can run a recovery and the written steps are current.
- ❑ Confirm your backup tools and storage themselves are supported and not end-of-life.

Tie this to your insurance renewal or tax time so it lands on a schedule. A backup setup that was perfect two years ago can quietly fall behind a growing business — the yearly look catches that drift before it becomes a gap.

★ Glad to do the yearly review with you

Once a year I can sit down with you, check that your backup still covers everything that matters, confirm the offline copy, and update your recovery plan. One visit, real peace of mind. Call (330) 200-8042.

Common Questions

The questions owners ask me most about backups and testing them, answered plainly.

Q: How often should I really test a restore?

Quarterly — four times a year — is a solid rhythm for most small offices: restore a file, an email, and a whole machine each time, and log it. Also run a quick test before any big upgrade or after any change to the backup itself. The key is testing on a schedule, not just meaning to.

Q: Isn't my cloud service already backing everything up?

Not necessarily. Cloud services keep your data running and often have limited, short recovery for recently-deleted items, but that's not the same as a full backup you control. If an account were compromised or a whole mailbox lost, you may need your own backup of your cloud data to get it all back.

Q: What does it mean to keep a backup 'offline' or 'immutable'?

Offline means disconnected — unplugged or kept somewhere not reachable over the network, so ransomware can't touch it. Immutable means set up so that even an attacker can't change or delete it for a set time. Either way, it's the copy that survives an attack on everything else.

Q: The whole-machine restore sounds hard. Do I really need it?

Yes, because files alone don't get a dead computer working again. Testing a full restore to spare hardware or a test setup proves you could rebuild, and tells you how long it would take — your real downtime. It's the part most offices skip and most need. I'm glad to walk you through it.

★ Want to prove your backup actually works?

Give me a call and we'll run a real fire drill together — file, email, and a whole machine — so you know, not hope, that you could recover. Call or text (330) 200-8042.

Your next step, today

You don't have to overhaul anything. One small action this week tells you where you really stand.

Right now, try to restore a single file from your backup. Just one. Whether it takes thirty seconds or reveals that you're not quite sure how — or that the file isn't there — you'll have learned something real about your safety net, which is more than most businesses know about theirs. That one small test is the whole fire drill in miniature.

Then put a quarterly reminder on the calendar to run the full drill, make sure one backup copy is offline or protected from ransomware, and start a simple log. That's the entire program — and it's the difference between hoping you're covered and knowing it.

✓ One restored file today is worth more than good intentions

The gap between businesses that recover and businesses that don't usually isn't the backup software — it's whether anyone ever tested it. Restore one file this week and you've already crossed to the right side of that line.

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 testing your backups 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.

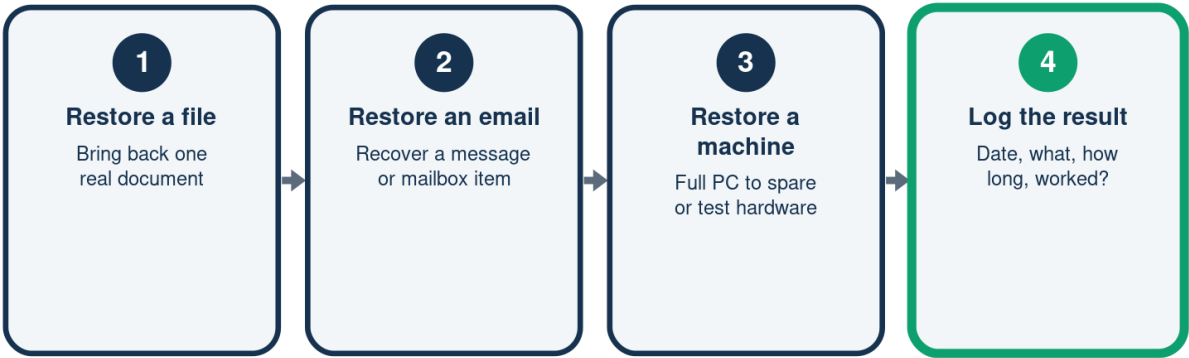
When you'd rather have a hand, that's exactly what I do. I come to your business, work at your pace, and never make you feel rushed or silly for asking. A first visit is a flat \$99, and for the parts that don't need me on-site I can often help right on your screen for \$49. Every visit comes with a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

The Quarterly Fire Drill

Prove you can actually restore



A backup isn't real until you've restored from it.

The 3-2-1 Idea

Don't let one event reach every copy

	What it means	Why it helps
3 copies	Working + 2 backups	One can fail
2 kinds	Different storage	One flaw misses one
1 offsite	Offline or elsewhere	Survives disaster
1 untouchable	Offline/immutable	Survives ransomware

The offsite, offline copy is the hero of the rule.

The Restore Log

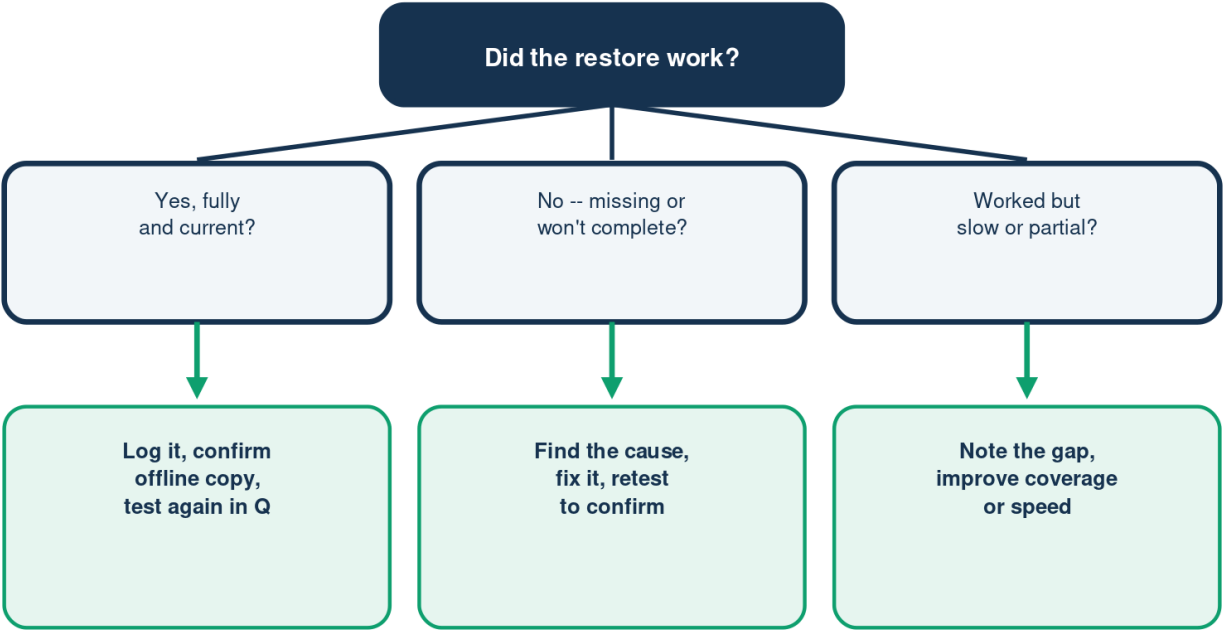
One line per test does a lot

Log this		Why it matters
Date tested	Proves it's current	Answers insurers
What restored	Shows coverage	File/email/machine
Worked?	Flags problems	Before a disaster
How long	Your real downtime	Plan around it

A dated log turns 'tested backups' into an honest, provable yes.

A Restore Test -- What Now?

Every outcome moves you forward



A failed drill today prevents a failed recovery after a real disaster.

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