



An Extended Guide · No. 2083

Encrypting Office Laptops: BitLocker & FileVault Before One Goes Missing

Turn on disk encryption and save the
recovery key where you'll find it

Tech Made Simple — Service Made Personal

BillsHomeTech.com · (330) 200-8042 · Atwater, Ohio

Free & printable — share it with someone who needs it



Book a visit —
billshometech.com/book

! Read this first — the two things that stop most attacks

Almost every small-business break-in starts in one of two ordinary ways: a password that got stolen or guessed, or a convincing email that talked someone into clicking or paying. You do not have to become a computer expert to stop most of it. Turn on two-step sign-in (also called multi-factor authentication, or MFA) everywhere you can, keep a backup you have actually tested, and give yourself permission to slow down before you click a link, open an attachment, or send a payment. That is the whole game, most days. There's one more quiet safeguard worth an afternoon: turning on disk encryption, so that if a laptop is ever lost or stolen, the data on it is unreadable to whoever ends up with it.

Before one of your laptops goes missing

A laptop gets left in a coffee shop, slips out of a bag at the airport, or walks off from a job site. It happens to careful people. The question is whether the stranger who finds it can read your files — your customer list, your invoices, your saved passwords — or just hits a wall. Encryption is that wall, and both Windows and Mac have it built in.

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. Encryption sounds like a word for spies; it's really just a switch most of your computers already have, waiting to be turned on.

Here's the whole idea in one breath: encryption scrambles everything on the drive so it can only be unlocked with your sign-in — or, in a pinch, a **recovery key**. Turn it on, save that recovery key somewhere safe, and a lost laptop becomes an expensive paperweight to a thief instead of a breach you have to report.

★ I'll turn it on and save the keys where you'll find them

The setup is quick; the part people get wrong is the recovery key. I can switch encryption on for every office laptop and store each key somewhere safe and separate, so you're protected without risking a lockout. Call or text me at (330) 200-8042.

The whole guide, on one page

If you remember only these things, your laptops are in good shape.

- ❑ **BitLocker** encrypts Windows laptops (Pro and Business editions); Windows Home has **Device Encryption** on supported hardware.
- ❑ **FileVault** encrypts Macs. Same idea, one switch in Settings.
- ❑ Encryption makes a lost or stolen laptop's data **unreadable** to anyone who doesn't have your sign-in.
- ❑ The **recovery key is everything**. Save it somewhere safe AND separate from the laptop before you need it.
- ❑ Good places for the key: your Microsoft or Apple account, a printout in a safe, or your password manager — ideally more than one.
- ❑ Do it on every laptop that leaves the building, and note which machines are encrypted so you can prove it later.

! Lose the recovery key and you can lose the data

Encryption protects the drive from everyone — including you, if you get locked out and can't produce the recovery key. A forgotten key after a failed update or a dead sign-in can mean the files are gone for good. Save the key in two safe places the day you turn encryption on.

What encryption actually does (and doesn't)

It helps to know exactly what you're getting, so you don't expect the wrong kind of protection.

Disk encryption scrambles everything stored on the laptop's drive into gibberish. When you sign in normally, the computer unscrambles it on the fly and you never notice. But pull the drive out, or try to boot it without the right sign-in, and all a thief sees is noise. Your data is safe **at rest** — when the machine is off or locked.

What it does **not** do is protect a laptop that's already unlocked and sitting open, or stop someone who knows your password, or keep out a scam email. Encryption is one layer — the layer for lost and stolen hardware. You still need a strong sign-in, two-step verification, updates, and backups. Think of encryption as the deadbolt, not the whole security system.

✓ A screen lock and a strong password still matter

Encryption does its job when the machine is locked or off, so set it to lock the screen quickly and require a real password or PIN to wake. An encrypted laptop left open and unlocked on a counter is still wide open.

BitLocker: the Windows side

If your office runs Windows, BitLocker is the built-in tool — on the right edition.

BitLocker comes with Windows **Pro** and **Business** editions. You turn it on from Settings (search for 'BitLocker' or look under device encryption settings), choose to encrypt the drive, and Windows offers to save your recovery key. That recovery-key moment is the most important click in the whole process — don't rush past it.

Windows **Home** edition doesn't have the full BitLocker controls, but many Home laptops have **Device Encryption** — a simpler version that turns on automatically on supported hardware when you sign in with a Microsoft account. It's worth checking Settings to see whether it's already on. The exact menu names and paths change between Windows versions, so if yours look different, that's normal — check your current Settings.

✓ Not sure which edition you have?

Open Settings and look under 'System' then 'About' for the Windows edition, or just search the Start menu for 'encryption.' If you see BitLocker, you're on Pro or Business; if you see Device Encryption, you're likely on Home. Either one, turned on, is far better than a drive left in the clear.

FileVault: the Mac side

If your office runs Macs, FileVault is the one switch to find.

FileVault is Apple's built-in disk encryption. You turn it on in System Settings, under Privacy & Security (older Macs call it System Preferences). Flip it on, and the Mac encrypts the drive in the background while you keep working. As with Windows, the menu names may shift between macOS versions, so check your current Settings if the wording differs.

When you enable FileVault, the Mac asks how you want to be able to unlock the drive if you forget your password: using your **Apple account**, or with a **recovery key** it shows you once. Whichever you pick, that is your lifeline — write the recovery key down and store it safely, or make sure you'll always have access to that Apple account. Don't just click past this screen.

! Newer Macs are partly protected — but turn FileVault on anyway

Macs with Apple's security chips keep the drive tied to the machine, which helps, but FileVault is what makes the data truly unreadable without your sign-in. Turning it on is the step that lets you honestly say the laptop is encrypted — on an insurance form or to a worried customer.

The recovery key is everything

If you take one thing from this guide, take this: the recovery key is the master key to your encrypted drive, and losing it can mean losing your data.

When you turn on encryption, the computer generates a long recovery key — a string of numbers and letters. It's the backup way in if your normal sign-in ever fails: after a hardware change, a troubled update, a forgotten password, or a drive moved to another machine. Windows and Mac will both ask you to save it. That request is not a formality.

Here's the hard truth that catches good people off guard: because encryption keeps **everyone** out without the key, there is no locksmith, no back door, and no support line that can recover the data if both your sign-in and your recovery key are gone. The scrambling that protects you from a thief protects you from yourself just as completely.

! No key, no data — nobody can override it

This is the single most important warning in the guide. Save the recovery key the moment encryption asks for it, in a safe place that is NOT on the laptop itself. A laptop that locks you out with the key sitting in a drawer at the office is a recoverable annoyance; a laptop that locks you out with no key anywhere is a permanent loss.

Where to store the recovery key safely

Safe AND separate is the rule. You want the key easy for you to reach and impossible for a thief to find with the laptop.

The goal is at least two independent copies, kept away from the machine they unlock. If the only copy lives on the laptop, a thief has both the lock and the key — and if the laptop dies, so does your access. Spread the copies out so no single bad day wipes out all of them.

- **Your Microsoft or Apple account:** both offer to store the key tied to your account, so you can look it up from another device.
- **A printout in a safe or locked drawer:** old-fashioned, offline, and immune to a computer failure.
- **Your password manager:** a labeled entry per laptop keeps keys organized and behind your master password.
- **A sealed envelope with your important business papers:** for the owner's own machine, kept where you keep the insurance policy.

✓ Label each key with the laptop it belongs to

When you have more than one encrypted machine, an unlabeled key is nearly useless — you won't know which laptop it opens. Note the computer's name or a sticker number next to each key so there's no guessing in a crisis.

A couple of laptops, or a drawer full of them

The switch is the same everywhere, but how you manage the recovery keys depends a lot on how many machines leave your building.

If you have one or two laptops

With just a machine or two, you can turn encryption on this afternoon and keep the keys in your own hands. Keep it simple and personal — you're the one who'll be looking for that key if you ever need it.

- Turn on BitLocker or FileVault on each laptop today; it runs in the background while you work.
- Save each recovery key to your Microsoft or Apple account AND print a copy for your safe.
- Jot the laptop's name next to its key so you can tell them apart.
- Re-check once a year that encryption is still on and the keys are still where you put them.

If you have a team with several laptops

More machines means more keys to keep straight, and the real risk shifts from 'did I turn it on?' to 'can I find the right key for the right laptop when someone's locked out or a device walks off?' Treat key storage like the important record it is.

- Keep one organized list of every laptop, who uses it, and where its recovery key is stored.
- Prefer storing keys in your business accounts so they don't live only in one person's head.
- Make encryption part of setting up any new laptop — before it holds real data or leaves the office.
- When someone leaves, their laptop's encryption and key handling tie into your offboarding steps — our offboarding guide covers the rest.

★ I'll get every laptop encrypted and the keys organized

Whether it's two machines or a dozen, I can turn encryption on across the board, store the keys safely and separately, and hand you one simple list of what's protected and where each key lives. Call (330) 200-8042.

A calm way to turn it on

Encryption on a laptop that already has your files is safe to turn on, but a little care makes it painless.

- ❑ Back up the important files first — just in case, the way you would before any big change.
- ❑ Make sure the laptop is plugged in; the first encryption pass can take a while and you don't want it to stop halfway.
- ❑ Turn on BitLocker (Windows) or FileVault (Mac) from Settings.
- ❑ When it asks where to save the recovery key, save it to your account AND print or copy it somewhere separate — do this now, not later.
- ❑ Let it finish encrypting in the background; you can keep working.
- ❑ Write down that this laptop is now encrypted and where its key lives.

✓ Back up before you start — always

The chance of trouble is small, but the cost of trouble on an un-backed-up machine is high. A current backup turns any surprise into a shrug. Our backup fire-drill guide shows how to be sure that backup actually works.

Home edition, old laptops, and the gaps

Not every machine encrypts the same way, and a few won't do it at all. Here's how to spot the gaps.

Windows **Home** edition can usually do **Device Encryption** on newer hardware, but some older Home laptops don't support it. If yours can't, you have a choice: upgrade that machine to Windows Pro (which adds full BitLocker), or decide that laptop simply shouldn't carry sensitive data off-site. Both are fine answers — the wrong answer is assuming it's encrypted when it isn't.

Very old laptops may lack the small security chip (often called a TPM) that makes encryption smooth, or may be too slow to encrypt comfortably. If a machine is both old and carrying customer data out of the building, that's a sign it's due for replacement — which also ties into keeping your software supported, covered in our updates-and-end-of-support guide.

✓ Check, don't assume

The only way to know a laptop is encrypted is to open Settings and look. A machine you think is protected but isn't is worse than one you know is open, because you'll answer 'yes' on forms and to customers based on a guess.

The day a laptop actually goes missing

This is the moment encryption earns its keep. What you do — and what you don't have to do — changes completely.

If an **encrypted** laptop disappears, the data on it is unreadable to whoever has it, as long as it was locked or off and your sign-in is strong. That often means you're dealing with the cost of replacing hardware, not the far bigger cost and stress of a reportable data breach. You still change the passwords for any accounts that were signed in on it, and you still report the loss, but the customer data stays protected.

If an **unencrypted** laptop disappears, you have to assume whoever has it can read everything — and that can turn a lost device into a notification obligation and a very bad week. Our offboarding and lost-device guide walks through the steps for a missing machine; encryption is what keeps that checklist short.

! Encryption can be the difference between a loss and a breach

The same stolen laptop is either a replaceable piece of hardware or a headline, depending on one switch you flipped weeks earlier. That is the entire case for turning encryption on before you ever need it.

Phones, tablets, and personal devices

Laptops aren't the only thing that walks off. A quick word on the pocket-sized risks.

Modern phones and tablets encrypt themselves automatically once you set a PIN, passcode, or fingerprint/face unlock — so the most important thing you can do there is simply require a real screen lock, not leave it wide open. If staff read work email or files on their own phones, that lock is doing the encrypting for you.

When people use personal laptops or home PCs for work, you can't always force encryption the way you can on a company machine. That's one reason a short written rule for personal devices matters — screen lock, updates, and the ability to cut off work access if a device is lost. Our guide on personal devices at work (BYOD) covers that policy in plain English.

✓ A screen lock is the phone's encryption switch

On a phone, 'turn on encryption' really means 'set a passcode and use it.' No passcode, no encryption. Make a real lock the baseline for any device that touches work email or files.

What your insurer and your forms want to see

Encryption shows up on cyber-insurance applications and security checklists, and it's an easy, honest 'yes' to earn.

Many cyber-insurance applications ask whether laptops and portable devices are encrypted, because insurers know a lost encrypted laptop usually isn't a payout. Answering 'yes' truthfully can help your application — but as our cyber-insurance application guide stresses, the answer has to be **true for every machine** they're asking about, not just most of them.

There's a legal angle too: breach-notification rules often don't require you to notify people when the exposed data was **encrypted**, because encrypted data isn't readable. That's a general principle, not legal advice — the details depend on your situation and state — but it's one more reason encryption pays for itself.

! 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.

The mistakes that undo good intentions

Encryption is simple to get right and easy to quietly get wrong. Here are the slips I see most.

- **Storing the recovery key on the laptop itself** — which hands a thief both the lock and the key.
- **Clicking past the 'save your recovery key' screen** and meaning to come back to it (you won't).
- **Assuming a Home-edition laptop is encrypted** without checking whether Device Encryption is actually on.
- **Only one copy of the key**, so a lost printout or a closed account locks you out for good.
- **Leaving the laptop unlocked** all day, so the encryption never actually engages.
- **No record of which machines are encrypted**, so you can't honestly answer a form or a customer.

! The recovery-key mistakes are the costly ones

Almost every encryption horror story comes down to a recovery key that was never saved, saved in only one place, or saved on the very machine it was meant to rescue. Get the key right and the rest is easy.

Common worries, put to rest

Owners hesitate to turn encryption on for a few reasons that mostly don't hold up anymore.

'Won't it slow my laptop down?' On modern machines the difference is so small you won't notice it in day-to-day work. The hardware handles the scrambling behind the scenes. The one-time first encryption pass takes a while, but you can keep working through it.

'What if it breaks my computer?' Encryption is a mature, built-in feature used by millions of businesses; it doesn't harm your files. The real risk isn't the encryption — it's losing the recovery key, which is entirely in your control. Back up first, save the key in two places, and you've removed the only genuine danger.

'We're too small to be a target.' Lost and stolen laptops aren't targeted attacks — they're accidents and petty theft that happen to small shops constantly. Encryption protects you from the ordinary bad day, not just the master hacker.

✓ The cost is a few minutes; the payoff is a disaster avoided

Weigh a few minutes of setup and a saved key against the cost of a reported breach, lost customer trust, and the scramble to notify everyone. It's one of the best trades in all of small-business security.

Keep a simple record of what's protected

A one-page list turns 'I think so' into 'yes, here's the proof' — for you, your insurer, and your own peace of mind.

For each laptop, note the machine (a name or sticker number), who uses it, whether encryption is on, and where its recovery key is stored. That's it. Keep the list with your other business records — not only on one of the laptops — and update it whenever you add or retire a machine.

On your list	Why it's there
Laptop name / number	So a key maps to the right machine
Who uses it	So you know whose access to cut if it's lost
Encrypted? yes/no	So you can answer forms honestly
Where the key lives	So you're never hunting during a crisis

✓ **This pairs with your one-page security plan**

If you keep the simple security plan from our one-page plan guide, add an encryption column to it. One living page covering accounts, backups, and encrypted devices is worth more than a thick binder nobody opens.

Before you sell, donate, or retire a laptop

Encryption also helps at the end of a laptop's life — if you handle the hand-off right.

When a laptop leaves your hands for good, the safest path is to erase it properly — use the built-in 'reset and remove everything' or erase-all option, which on an encrypted machine effectively throws away the key and makes the old data unrecoverable. Sign out of your accounts first, and make sure you've moved anything you still need off the machine.

Don't just drag files to the trash and call it done; that leaves data behind. And once you've wiped a machine, cross it off your encrypted-device list so your records stay accurate. If a drive is truly dead and can't be wiped, physically destroying it is the sure way to retire it.

! A traded-in laptop can leak more than a stolen one

People are careful about theft but casual about trade-ins and donations — and an old laptop handed off with its data intact is a slow-motion breach. Wipe every machine before it leaves, every time.

What about desktops and the office server?

Encryption isn't only for the machines that travel — but the priority is different.

The biggest payoff from encryption is on anything that **leaves the building**, because that's what gets lost or stolen. Laptops come first, every time. But desktops and small servers can be stolen in a break-in too, so encrypting them is a reasonable next step, especially if they hold customer or financial records in an office that isn't always staffed.

Servers and shared storage can be more involved to encrypt without locking yourself out, so that's a good one to plan rather than rush. The same rule rules everything: wherever you turn encryption on, save the recovery key somewhere safe and separate **first**.

✓ Start with what travels, then work inward

A simple order of operations: encrypt every laptop, then desktops that hold sensitive data, then plan the server with a little more care. You get most of the protection from the first step.

A two-minute yearly check

Encryption is close to set-and-forget, but a quick yearly look keeps it honest.

- ❑ Open Settings on each laptop and confirm encryption still shows as on.
- ❑ Confirm each recovery key is still where your list says it is — and that you can actually get to it.
- ❑ Add any new laptops bought during the year, and remove any you retired.
- ❑ Check that new staff laptops got encrypted before they started carrying real data.
- ❑ Make sure keys aren't tied only to an account or a person who has since left.

Tie this to something you already do once a year — renewing your insurance, doing taxes, or your backup review — so it actually happens. A couple of minutes per machine keeps your 'yes, we encrypt' both true and provable.

★ I can do the yearly check with you

If keeping track feels like one more thing, I'm glad to run the yearly encryption-and-key check as part of a visit, and leave you with an updated list. Call (330) 200-8042.

Where encryption fits in the bigger picture

Encryption is one strong layer. It works best alongside the other simple habits we talk about across these guides.

Picture the layers: two-step sign-in keeps people out of your accounts; a tested backup means you can recover from almost anything; updates close the holes attackers use; and encryption makes sure a lost or stolen machine doesn't hand over your data. No single one is enough, but together they stop the vast majority of what goes wrong at a small office.

The nice thing about encryption specifically is how little it asks of you after setup. Turn it on, save the keys, keep the list current — and then it quietly protects you for years, with no daily effort and nothing to remember.

✓ One layer at a time is fine

You don't have to do everything this week. If encryption is the layer you haven't turned on yet, start there — it's one of the quickest wins, and it pairs naturally with the backup and sign-in habits in our other guides.

Common Questions

The questions owners ask me most about encrypting their laptops, answered plainly.

Q: If I turn on encryption, will I have to enter the recovery key every day?

No. Day to day you just sign in the way you always have. The recovery key is only for unusual situations — a hardware change, a troubled update, or a forgotten password. That's exactly why it's easy to forget you saved it, so store it safely up front.

Q: I have a mix of Windows and Mac laptops. Is that a problem?

Not at all. Use BitLocker (or Device Encryption) on the Windows machines and FileVault on the Macs — same idea, two switches. Just keep one list that covers both so no machine slips through.

Q: What if I already lost a laptop that wasn't encrypted?

Treat it as if the data could be read: change the passwords for any accounts that were signed in on it, and follow the steps in our offboarding and lost-device guide. Then encrypt the rest of your machines so the next lost laptop is just lost hardware.

Q: Is encryption enough on its own?

No — it protects lost and stolen machines, but you still need strong sign-ins, two-step verification, tested backups, and current updates. Encryption is one important layer, not the whole wall.

★ Want a hand getting it all turned on?

I can encrypt every laptop you've got, save the keys safely and separately, and leave you with a simple list of what's protected. Call or text (330) 200-8042.

You don't have to do this alone

You just have to remember that a friendly, patient person is one call away.

I hope this guide made encrypting your office laptops 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

BitLocker vs FileVault, at a Glance

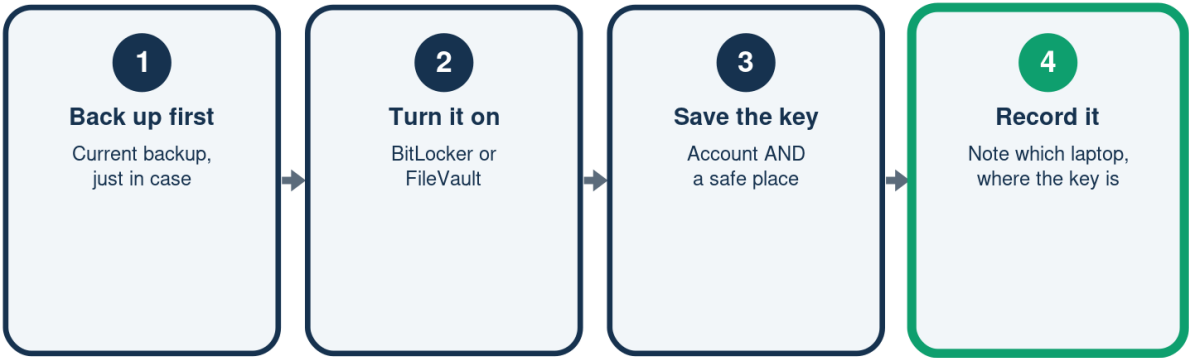
Same job, one switch on each platform

	BitLocker (Windows)	FileVault (Mac)
Built into	Windows Pro/Biz	macOS
Home edition	Device Encryption	N/A -- all Macs
Turn on from	Settings	System Settings
Recovery key to	Microsoft account	Apple account
The key rule	Save it separate	Save it separate

Either one, turned on, makes a lost laptop's data unreadable.

Turning Encryption On

The calm, no-lockout way



Saving the recovery key is the step you cannot skip.

Where to Keep the Recovery Key

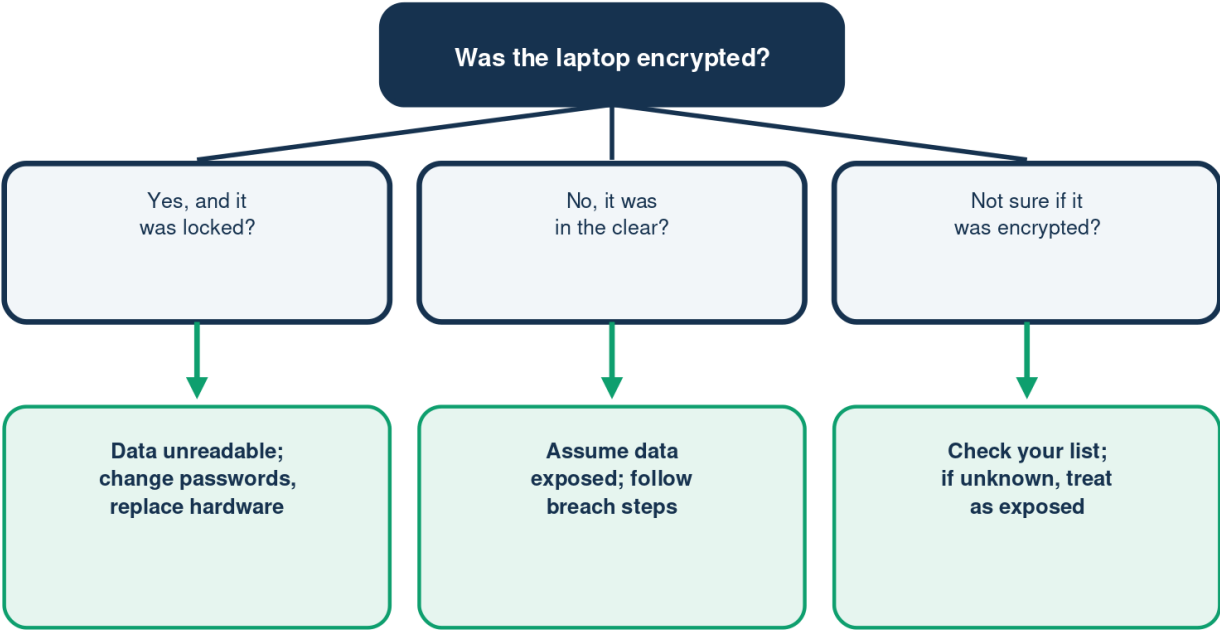
Safe and separate from the laptop

	Place	Good because
MS/Apple account	Reachable	from elsewhere
Printout in safe	Offline,	no screen needed
Password manager	Organized,	behind one key
On the laptop	NO -- thief gets	lock and key

Keep at least two copies, never only on the machine itself.

A Laptop Goes Missing -- Now What?

Encryption decides how bad the day is



This is why you turn encryption on before a laptop ever goes missing.

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