



Hardware Security Keys (YubiKey) for the Cautious

The little key that locks down your accounts

————— An Extended Guide · No. 1650 · PASSWORDS & SECURITY —————

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.

1. What a security key actually is	4
2. Who a security key is really for	4
3. How signing in with a key feels	5
4. FIDO2 and passkeys, in plain words	5
5. Choosing the right key for your devices	6
6. Why you should buy two keys	6
7. Which accounts accept a security key	7
8. Setting up your first key, step by step	7
9. Registering a backup — and keeping recovery codes	8
10. What happens if you lose a key	9
11. Using a key with your phone	9
12. Keys versus authenticator apps versus texts	10
13. Buying safely and avoiding fakes	10
14. Keeping your key in good shape	11
15. Common worries, answered	11
16. A simple plan to get started	12
17. Adding a key to your Google account	12
18. Adding a key to your Microsoft account	13
19. Protecting your password manager with a key	13
20. Two kinds of keys you'll see	14
21. Keys and your Apple devices	14

22. What a security key does not do	15
23. Traveling with a security key	16
24. Setting up a key for a parent	16
25. A once-a-year check	17
26. Keys at home and at work	17
27. What the little light and tap mean	18
28. Keys, passwords, and the password manager together	18
29. Explaining a security key to family	19
30. A security key for a small home office	19
31. When a visit makes sense	20
Your Security-Key Cheat Sheet	20
Plain-English Word List	21
A Picture to Follow Along	23
A Second Look	24
A Note From Bill	24
Your Visit — and My Promise	25

1. What a security key actually is

A little device that proves it's really you.

A security key is a small gadget, about the size and shape of a short house key or a thick thumb drive, that you keep on your keyring or in a drawer. When you sign into an account that's protected by one, the website asks you to insert the key into your computer, or tap it to your phone, and give it a touch. That single touch is proof that you — the real you, holding the real key — are the one signing in.

What makes it special is that there's nothing for a crook to steal from a distance. There's no code to read aloud, no password to type into a fake page, no text message to intercept. The secret lives inside the key and never leaves it. A scammer on the other side of the world can have your password and still be stopped cold, because they don't have the little key sitting on your desk.

GOOD TO KNOW

You don't need to understand the technology to use it. If you can plug in a flash drive or tap a card to pay, you can use a security key.

2. Who a security key is really for

Not everyone needs one — but if you want the strongest lock, this is it.

A security key is the most protective second step you can put on an account, and it's especially worth it for a handful of high-value logins: your main email, your password manager, your bank and investment accounts, and anything tied to your money. If a thief can't get into those, most other trouble is out of reach.

It's a great fit for anyone who likes the idea of a physical lock they can hold, who worries about being tricked online, or who manages money and wants real peace of mind. It's also a thoughtful gift for a parent, because once it's set up it just works — there's no app to fuss with.

- Best for: email, password manager, bank, and investment logins.
- Great for people who prefer a physical key over phone codes.
- A solid choice if you've been targeted by scams before.

WATCH OUT

You don't have to protect every account with a key. Put one on your two or three most important logins and you've covered the doors that matter most.

3. How signing in with a key feels

Three moves, then you're in.

The first time, you'll wonder what the fuss was about — it's genuinely easy. You type your username and password as usual. Then, instead of waiting for a text, the site asks for your key. You insert it into a USB port, or hold it against the back of your phone, and touch the little metal disc on it. A light blinks, the site accepts it, and you're in.

- 1 Enter your username and password as normal.
- 2 When the site asks for your key, insert it or tap it to your phone.
- 3 Touch the key's sensor when it lights up.
- 4 That's it — you're signed in.

The whole thing takes a few seconds, and there's nothing to read, type, or remember. Many people find it faster and calmer than hunting for a texted code before it expires.

4. FIDO2 and passkeys, in plain words

You'll see these words — here's what they mean to you.

When you shop for a key or set one up, you'll bump into a few technical words. You don't need to master them, but a plain translation helps you feel confident. FIDO2 and WebAuthn are simply the modern standard that makes keys work safely across websites. When a site says it supports security keys or passkeys, that's the good, phishing-proof kind at work.

A passkey is the newer idea of signing in without a password at all, using something you have — like your phone or your security key — plus a touch or a glance. A modern security key can store passkeys, so it can serve both as a strong second step on top of a password and, on sites that allow it, as the whole sign-in by itself.

GOOD TO KNOW

Older keys offered only one-time codes. Newer keys do the modern, phishing-proof kind. When buying, look for a key that lists FIDO2 or passkey support, which the common all-rounders all do.

5. Choosing the right key for your devices

The main thing is matching the plug to your gadgets.

Security keys come in a few shapes so they fit different devices. The only real decision is making sure the key's connector matches the ports on the computer and phone you'll use it with. If you mix an older computer and a newer phone, look for a key that covers both.

- USB-A — the older, wider rectangular plug on many desktops and older laptops.
- USB-C — the smaller, oval plug on newer laptops, Macs, and Android phones.
- NFC — tap-to-connect, for holding the key against the back of a phone.
- Lightning — the older iPhone plug, on keys made to suit those iPhones.

A popular, flexible choice is a key that has a USB-C plug and also does NFC tapping, which covers a newer laptop and most phones in one device. If you're unsure which ports you have, I'm glad to help you pick before you buy.

TIP

Check your computer's ports first. If the plugs look wider and rectangular, you want USB-A; if they're small ovals, you want USB-C.

6. Why you should buy two keys

The single most important rule in this whole guide.

Here's the rule that saves people the most grief: always buy two keys, not one. You'll use one day to day and lock the other away as a spare. Then you register BOTH keys on each important account. That way, if your everyday key is ever lost, broken, or left in a coat pocket on a trip, your spare still gets you in.

A security key is wonderfully secure precisely because no one else can get in without it — which is also why a single key with no backup is a risk to you. Two keys turn that risk into a non-event. Losing one becomes a minor errand to buy a replacement, not a lockout.

WATCH OUT

Never register just one key and stop. If it's your only key and it's lost, you can be locked out of the very accounts you were trying to protect. Two keys, always.

Keep the spare somewhere safe and separate — a home lockbox, a safe, or a trusted drawer — not on the same keyring as the first.

7. Which accounts accept a security key

More than you'd think — and the important ones are covered.

Support for security keys has grown a great deal, and the accounts most worth protecting are generally on board. Google and Microsoft accounts both accept security keys. Apple accounts support security keys as well. Many password managers let you protect your vault with one, and a long list of other services — social media, some banks, and more — accept them too.

- Google and Microsoft personal accounts — well supported.
- Apple accounts — security keys are supported.
- Password managers — many let a key guard the vault.
- A growing list of banks, social networks, and other services.

Because the list keeps changing, the simplest approach is to check each account's own Security or Sign-in settings and see whether 'security key' or 'passkey' appears as an option. If it does, you can add your key there.

GOOD TO KNOW

Not every account offers keys yet. For those, an authenticator app is the next-best second step, and you can still cover your top accounts with a key.

8. Setting up your first key, step by step

The same shape on almost every site, so you'll learn it once.

Setting up a key is a one-time task per account, and the steps rhyme from site to site. Do it on a computer when you can — it's roomier than a phone screen. Have both keys in hand before you start, so you can register them back to back.

- 1 Sign into the account on a computer.
- 2 Open its settings and find Security or Sign-in.

- 3 Look for 'security key,' 'passkey,' or 'two-step verification.'
- 4 Choose to add a security key.
- 5 Insert your key and touch it when it lights up.
- 6 Give it a name you'll recognize, like 'blue key.'
- 7 Repeat with your second key right away.

When both keys are listed in the account's settings, you're done. Take a moment to confirm you also still have a backup method and your recovery codes saved, which the next chapters cover.

TIP

Naming your keys ('blue key,' 'spare in safe') makes the settings page easy to read later, so you always know which key is which.

9. Registering a backup — and keeping recovery codes

Belt and suspenders, so a lost key is never a disaster.

A security key is strong, so your backups matter. Three simple habits keep you from ever being locked out. First, register your second key on every account that holds the first. Second, keep at least one other sign-in method available where the site allows it, such as an authenticator app. Third, save the recovery codes each account offers.

- Both keys registered on every important account.
- One backup method kept active where offered.
- Recovery codes saved in your password manager or a safe place.

Recovery codes are short one-time codes a site gives you at setup. They're your emergency way in if you somehow lose both keys. Treat them like cash: store them somewhere safe and don't share them.

WATCH OUT

Don't leave your recovery codes in an email or a note on your desk. A password manager or a locked drawer is the right home for them.

10. What happens if you lose a key

With a spare, it's a small errand — not a crisis.

Say your everyday key goes missing. Because you registered a second key, you simply sign in with the spare and carry on. Then, when you have a calm moment, you go into each important account and remove the lost key from its list, so it can't be used by whoever might find it. Finally, you buy a new key and register it as your fresh spare.

- 1 Sign in with your backup key.
- 2 In each account's security settings, remove the lost key from the list.
- 3 Order a replacement key.
- 4 Register the new key so you're back to two.

A finder can't do anything useful with a lost key on its own — they'd also need your password and to know which accounts it unlocks. Removing it from your accounts closes the door completely.

GOOD TO KNOW

This is exactly why two keys matter. With a spare, losing one is a minor inconvenience instead of a lockout.

11. Using a key with your phone

Tapping is as easy as paying with a card.

Many keys can work with a phone, either by plugging into the phone's port or by tapping. The tap method, called NFC, is the same motion as holding a card to a card reader to pay. You bring the key to the back of the phone, hold it for a second, and the sign-in completes.

On an iPhone or Android phone, when a site or app asks for your key, you'll see a prompt to insert or tap it. Hold the key flat against the upper back of the phone until it registers. If tapping doesn't catch, try moving the key slowly around that area, since the tap spot varies by phone.

TIP

If your phone has a case, a thick one can make tapping fussier. Holding the key firmly against the back, or briefly removing a bulky case, usually does the trick.

12. Keys versus authenticator apps versus texts

Where a key fits among the second-step options.

There are three common ways to add a second step to a login, and they're not equally strong. A texted code is better than nothing, but it can be phished or stolen through a SIM-swap scam. An authenticator app, which makes codes on your phone, is better, because a SIM-swap can't reach it. A security key is the strongest of all, because there's no code to phish at all.

- Texted code — convenient, but the weakest; can be tricked or intercepted.
- Authenticator app — a solid, free step up from texts.
- Security key — the strongest; phishing simply doesn't work against it.

A sensible plan is a security key on your two or three most important accounts, an authenticator app on the rest, and texts only as a last-resort fallback where nothing else is offered.

GOOD TO KNOW

My guide comparing authenticator apps, texts, and email walks through the everyday choice in more detail if you'd like the full picture.

13. Buying safely and avoiding fakes

A few minutes of care at purchase time pays off.

A security key is a trust device, so buy it from a trustworthy source. The safest routes are the maker's own website or a major, well-known retailer. Avoid unknown third-party sellers offering suspiciously cheap keys, since a tampered or counterfeit key defeats the whole purpose.

- Buy from the maker's official site or a major retailer.
- Be wary of unknown sellers and prices that seem too good.
- Check the packaging looks sealed and genuine when it arrives.

The common all-rounder keys are modestly priced for what they protect — think of it as a small one-time cost for a lock on your most valuable accounts. Buying two from a reputable source is money well spent.

WATCH OUT

If a listing can't say clearly who makes the key, or the price is far below the maker's own, pass it by. For something this important, stick to sources you trust.

14. Keeping your key in good shape

They're tough, but a little care goes a long way.

Security keys are built to live on a keyring, so they shrug off everyday bumps, pocket lint, and the odd splash. Still, a few gentle habits keep yours reliable for years. Keep it away from extreme heat, don't let it rattle loose and get lost, and give the metal contact a wipe if it ever looks grimy.

- Keep your everyday key somewhere you won't misplace it — a keyring works well.
- Keep the spare separate, in a safe or lockbox.
- Avoid leaving a key in a hot car or in standing water.

TIP

A key on your keyring is always with you and hard to forget. The spare's whole job is to stay put somewhere safe, so pick its home once and leave it there.

15. Common worries, answered

The questions folks ask before they commit.

A few worries come up again and again, and they all have reassuring answers. 'What if it breaks?' — that's what your spare is for, and keys are quite durable. 'Do I need internet on the key?' — no, the key itself needs no battery or signal; your device handles the connection.

'Can someone steal my accounts if they steal my key?' — not on its own; they'd also need your password and to know which accounts it unlocks, and you can remove a lost key from your accounts. 'Is it hard to set up?' — it's a few minutes per account, and I'm happy to do the first one with you.

GOOD TO KNOW

A security key has no battery to die and nothing to charge. It draws what little power it needs from the device you plug or tap it into.

16. A simple plan to get started

The whole thing, in a few calm steps.

Let's bring it together. Protecting your most important accounts with security keys is a small, one-time project with lasting payoff. Here's the plan from start to finish.

- 1 Decide which two or three accounts matter most — email, password manager, bank.
- 2 Buy two keys that fit your devices, from a trusted source.
- 3 Register BOTH keys on each of those accounts.
- 4 Save your recovery codes and keep one backup method.
- 5 Store the spare key somewhere safe and separate.

That's the entire job. Once it's done, your most valuable logins carry the strongest lock available, and a scammer with your password is left out in the cold.

TIP

If setting up the first account feels like one step too many, that's exactly the kind of thing I help folks with — in person or by screen-share — in well under an hour.

17. Adding a key to your Google account

The steps on one of the most common accounts.

Google accounts accept security keys, and setting one up follows the familiar shape. You'll do this on a computer, signed into your Google account. Look in the account's Security area for the section about how you sign in, where two-step verification and security keys live together.

- 1 Sign into your Google account on a computer.
- 2 Open the Security settings for your account.
- 3 Find the section about how you sign in, and choose to add a security key or passkey.
- 4 Insert or tap your key and touch it when prompted.
- 5 Name the key, then add your second key the same way.

Once both keys are listed, Google will ask for one when it wants to be sure it's you. The exact wording of the menus shifts over time, so if a label looks a little different from what's written here, look for the words 'security key' or 'passkey' and you'll be in the right place.

GOOD TO KNOW

Google also offers an Advanced Protection option for people who want the strongest settings, which leans heavily on security keys. It's more than most folks need, but it's there if you want it.

18. Adding a key to your Microsoft account

For email, Office, and your Windows sign-in.

A personal Microsoft account — the one behind Outlook.com email, Office, and your Windows sign-in — also accepts security keys. As with Google, you'll manage it from the account's security settings in a web browser, signed in as yourself.

- 1 Sign into your Microsoft account in a web browser.
- 2 Open its Security settings and look for sign-in or advanced security options.
- 3 Choose to add a new way to sign in, then pick security key or passkey.
- 4 Insert or tap your key and touch it.
- 5 Repeat for your second key.

Windows itself has a built-in feature, often called Windows Hello, that lets you sign into the computer with a PIN, fingerprint, or face. A security key complements that by protecting the Microsoft account those features connect to.

TIP

If you have a work or school Microsoft account, its security is managed by that organization's settings, so the steps can differ. Check with your workplace's tech support for those.

19. Protecting your password manager with a key

The single most valuable account to lock down.

If you use a password manager — and I hope you do — it holds the keys to everything else, so it's the account most worth protecting with a security key. Many managers let you require a key in addition to your master password, so even someone who learned your master password still couldn't open the vault.

Look in your password manager's security or two-factor settings for an option to add a security key or hardware key. Register both of your keys there. Just be sure to keep your recovery route for the manager safe too, since losing access to the vault would lock you

out of a great deal at once.

WATCH OUT

Before you add a key to your password manager, make sure you've saved its account recovery information somewhere safe. The vault is too important to risk a lockout.

With a key guarding the vault, your whole collection of passwords sits behind the strongest lock there is — a fitting home for your most sensitive information.

20. Two kinds of keys you'll see

The all-rounder and the simpler, cheaper one.

When you shop, you'll notice a maker often sells two families of keys. One is a full-featured all-rounder that does the modern phishing-proof sign-in plus several older tricks. The other is a simpler, less expensive line that does just the modern sign-in and nothing extra. For most people, the simpler line is plenty.

- All-rounder — does modern passkeys plus older code types; costs a bit more.
- Simpler line — does the modern, phishing-proof sign-in only; costs less.
- For everyday email, bank, and manager protection, the simpler line is fine.

The extra features on the all-rounder matter mostly to businesses and technical users. If you just want to lock down your important personal accounts, you can save a little and get the simpler model — in two, as always.

GOOD TO KNOW

Whichever family you choose, make sure it lists passkey or FIDO2 support, which both lines from the major maker do. That's the capability that matters for you.

21. Keys and your Apple devices

How security keys fit the Apple world.

Apple accounts support security keys, and you can add them to strengthen how your Apple account signs in. You'll manage this in your device's settings, under your name and the sign-in and security area. As elsewhere, the menu wording can shift over time, so look for the option that mentions security keys.

Because Apple devices lean heavily on Face ID, Touch ID, and passkeys stored in your Apple account, many Apple users are already enjoying passwordless sign-ins without a separate key. A physical key adds an extra, hold-in-your-hand layer for those who want the strongest protection on the Apple account itself.

TIP

On Apple devices, a key that supports NFC tapping or has the right plug for your iPhone and Mac makes the experience smoothest. When in doubt, a USB-C key that also taps covers most newer Apple gear.

22. What a security key does not do

Knowing its edges keeps your expectations right.

A security key is the strongest lock on a sign-in, but it isn't a cure-all, and it helps to know what it doesn't cover. It protects the moment of logging in. It doesn't protect you if you hand money to a scammer over the phone, click a bad link that installs trouble, or share your screen with someone you shouldn't.

- It locks the front door of an account — it doesn't stop every scam.
- It won't help if you're talked into sending money or gift cards.
- It won't undo malware from a bad download.
- It only protects the accounts you actually add it to.

Think of a key as one excellent layer among several. Paired with good habits — pausing before you click, never sharing codes, and keeping software updated — it makes your most important accounts remarkably hard to break into.

GOOD TO KNOW

The biggest threat a key stops is phishing — being tricked into signing into a fake page. That alone makes it one of the best protections you can buy.

23. Traveling with a security key

A little planning keeps you covered on the road.

A security key travels well — it's small, needs no charging, and survives a suitcase. The one thing to plan is your backup. If you take your everyday key on a trip, keep your spare safely at home, and make sure you also have your recovery codes somewhere you can reach them if the worst happens far from home.

- Carry your everyday key; leave the spare safe at home.
- Keep recovery codes reachable in your password manager.
- A key that taps over NFC is handy when you only have your phone.

WATCH OUT

Don't pack both of your keys in the same bag. If the bag is lost, you'd lose both at once — the very thing two keys are meant to prevent.

With your everyday key in your pocket and your spare and recovery codes safe at home, you can sign into your accounts from anywhere with confidence.

24. Setting up a key for a parent

A thoughtful, low-fuss gift of protection.

A security key can be a wonderful thing to set up for an aging parent, because once it's in place it simply works — there's no app to open, no code to find, no password to recall beyond the one they already use. You can do the setup together on a visit, registering both keys on their email and bank.

Keep the spare key with your own records, or somewhere the family agrees on, and write down plainly which accounts the keys protect and where the recovery codes live. That way the protection doesn't depend on any one person remembering how it all works.

- Register both keys on their most important accounts together.
- Keep the spare and recovery codes with the family's records.
- Write a simple note of what's protected and how to get help.

TIP

Pair this with my guide on sharing passwords safely with a spouse or caregiver — it covers exactly where to keep these logins so the right people can reach them.

25. A once-a-year check

Five minutes to be sure everything's still in order.

Security keys need almost no upkeep, but a quick yearly look keeps you confident. Tie it to something you already do each year so it's easy to remember, and run through a short list to confirm your protection is intact.

- 1 Confirm both keys still appear in each important account's settings.
- 2 Check that your spare key is where it should be.
- 3 Make sure your recovery codes are still saved and readable.
- 4 Give each key a quick test sign-in so you know it works.

That's the whole routine. In a few minutes you've confirmed that the strongest lock on your most valuable accounts is still doing its quiet job.

GOOD TO KNOW

Testing both keys once a year catches the rare dud or a key you forgot to register somewhere, long before it could ever become a lockout.

26. Keys at home and at work

The same device, two slightly different worlds.

The keys you use for your personal accounts work the same way at a workplace, but a business often manages its own sign-ins and may hand out keys or set its own rules. If you use a key for both, you can register the same key on personal and work accounts, though it's often tidier to keep a dedicated key for work.

If you run a small business yourself, security keys are an excellent way to protect your email, your banking, and your point-of-sale or bookkeeping logins. The same two-keys rule applies, and it's worth making sure a trusted second person can get in if you're unavailable.

TIP

For a small business, I can help set up keys across your important accounts and make sure there's a safe backup plan — one of the common jobs I do with 30+ years of professional experience behind me.

27. What the little light and tap mean

A plain tour of how the key behaves, so nothing feels mysterious.

The first time you use a security key, the small blinking light and the gentle tap can feel unfamiliar. Here's what's happening. When a site asks for your key, you plug it into a USB port, or hold it to the back of your phone if it supports tapping. The light blinks to tell you it's waiting. You touch the metal contact — that touch is the key's way of knowing a real human is present — and in a second you're signed in.

That touch is the whole interaction. There's nothing to read, no code to type, no app to open. The key and the website quietly check each other behind the scenes, confirm it's the genuine site, and let you in. Once you've done it twice, it becomes as ordinary as turning a key in a lock.

- Plug in, or tap to the back of a phone.
- The light blinks — it's waiting for you.
- Touch the contact to prove you're there.
- You're in — no codes, no typing.

GOOD TO KNOW

Some keys ask you to set a PIN the first time. That PIN protects the key itself, so a lost key is useless to whoever finds it. Keep it with your other important numbers.

28. Keys, passwords, and the password manager together

A security key doesn't replace everything — it crowns it.

It helps to see where a security key fits in the whole picture. You still want strong, unique passwords for every account, and a password manager to remember them. The key sits on top of that, as the second factor — the proof that it's really you — on the handful of accounts that matter most. Think of the password as the lock and the key as the deadbolt you add to the most important doors.

In practice, most people protect their email, their password manager, and their main money accounts with the key, and let the manager plus an authenticator app cover everything else. That gives you phishing-proof protection exactly where a break-in would hurt most, without having to tap a key for every little login.

- Password manager — remembers the unique passwords.

- Security key — proves it's you on your most important accounts.
- Authenticator app — a good second factor on everything else.

GOOD TO KNOW

Your password manager can itself be protected by your security key. That single step guards the one vault that holds all the others.

29. Explaining a security key to family

A few plain comparisons that make it click.

If you want to bring a hesitant spouse or an adult child on board, you don't need technical language. A security key is just a house key for your online accounts. Nobody can sign in to a protected account without physically having that little key in hand — not a scammer in another country, not someone who guessed your password.

The part people find reassuring is that it can't be tricked. A fake login page can fool your eyes, but it cannot fool the key, because the key quietly checks that it's talking to the real website before it will work. That's why security experts consider it the strongest everyday protection there is.

- It's a physical key for your accounts.
- No key in hand means no sign-in — even with your password.
- It can't be fooled by a fake page, the way you or a code can.

TIP

Buying a pair of keys for a couple, and registering both on each other's key accounts, is a thoughtful and genuinely strong gift of security.

30. A security key for a small home office

If you run a little business from home, this matters more.

If you keep books, invoice clients, or store customer details on your home computer, your email and cloud accounts are the keys to your livelihood. A security key on those accounts is a small, one-time step that closes the door on the most common way small operators get hit — a phished password that lets a crook into the email and, from there, into everything.

The same two-key rule applies: register a primary and a backup, and keep the spare somewhere separate and safe. If you ever bring on help, each person should have their

own key rather than sharing one, so access stays clean and easy to manage.

- Protect the business email and cloud storage first.
- Keep a spare key off-site or in a safe.
- One key per person — never a shared login.

WATCH OUT

If you lose the only key to a business account and have no backup method set, you can be locked out of your own livelihood. The backup is not optional here.

31. When a visit makes sense

You don't have to do any of this alone.

There's no shame in wanting a hand with this. Choosing the right keys, registering both on your bank and email, saving the recovery codes, and practicing the tap until it feels ordinary — doing all of it in one calm sitting is one of the most satisfying little projects there is, and it keeps paying off for years.

If you'd like company for it, I do exactly this kind of setup all the time, with 30+ years of professional experience behind me. We can sit at your kitchen table or do it together over a screen-share, and I'll leave you with the cheat sheet by the computer.

GOOD TO KNOW

Bill's Home Tech serves Portage County and the surrounding area. Call or text (330) 200-8042 and Sophie or I can find a time that suits you.

CHEAT SHEET

Your Security-Key Cheat Sheet

Keep this by the computer. It's the short version of everything in this guide.

Before you buy

- Pick a key that fits your device's port (USB-C for newer, USB-A for older, NFC for tap).
- Buy TWO: one to use, one spare locked away.
- Buy from the maker's own site or a well-known retailer.

To set one up

- 1 Sign into the account on a computer.
- 2 Open its Security or Sign-in settings.

- 3 Choose to add a security key or passkey.
- 4 Insert or tap the key and touch it when it glows.
- 5 Add the SECOND key the same way, right then.

Keep yourself safe from lockout

- Register both keys on every important account.
- Keep one backup sign-in method and your recovery codes.
- Store the spare key somewhere safe, like a lockbox.
- Stuck? Call Bill's Home Tech at (330) 200-8042.

WORDS TO KNOW

Plain-English Word List

Security key — A small physical device you touch to prove it's you when signing in. Also called a hardware key.

YubiKey — A popular brand of security key, made by a company called Yubico. The 5 Series is the common all-rounder.

FIDO2 / WebAuthn — The modern standard that lets a security key sign you in safely. You don't need to remember the name — just that it's the good, phishing-proof kind.

Passkey — A sign-in that replaces your password, often stored on your phone or on a security key. A security key can hold passkeys.

NFC — Tap-to-connect, the same idea as tapping a card to pay. Lets a key work by holding it to a phone.

USB-A / USB-C — The two common plug shapes. USB-C is the smaller oval on newer devices; USB-A is the older rectangle.

Two-factor (2FA) — A second step after your password. A security key is the strongest kind of second step.

Recovery codes — One-time backup codes a site gives you to get in if you lose your other methods. Keep them safe.

Backup key — A second security key you register alongside the first, so losing one key never locks you out.

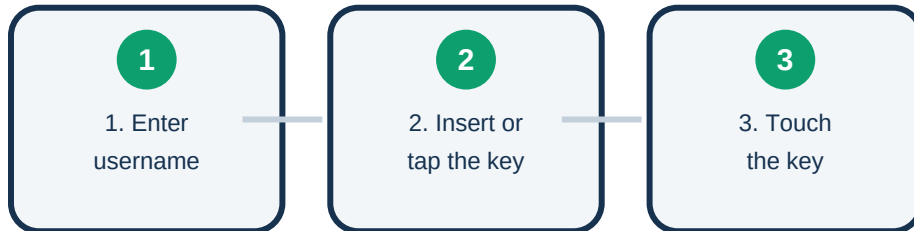
Phishing — A fake login page or message that tricks you into handing over your sign-in. A security key defeats it.

AT A GLANCE

A Picture to Follow Along

How a Security Key Signs You In

Three simple moves — no code to type, nothing to memorize.



That touch proves you're really there - and a crook across the world can't.

Illustration - a typical sign-in; some sites tap the key over NFC instead.

AT A GLANCE

A Second Look

Texted Code vs. Security Key

Both are a second step. One can be tricked; one really can't.

Texted Code	Security Key
- You read a number - Can be phished - SIM-swap risk - Works anywhere	- You touch a key - Phishing-proof - Nothing to steal - Needs the key

A security key is the strongest second step you can add to an account.

Illustration - a simplified comparison, not every detail of how sign-in works.

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

In-home visit — \$99 flat for your first visit. No contracts and no surprise charges, and a 30-day follow-up is included.

Remote Support — \$49 for a screen-share session. I only connect with your permission, you watch the whole time, and you can end anytime. If I can't fix it over the screen-share, I refund the \$49 — and if it turns out you need me in person, that \$49 goes toward your visit. It's included free for Support Plan members (\$39/mo).

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.

Call or text **(330) 200-8042** · Book a visit: **billshometech.com/book** · **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.