



An Extended Guide · No. 2082

Passkeys & Security Keys for Staff: Sign-Ins That Can't Be Phished

The strongest second step, and how
to roll it out to a few employees

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. This guide is about the strongest version of that second step: passkeys and security keys, which can't be phished at all, because they're tied to the real website and a fake login page captures nothing it could ever reuse.

Sign-ins that simply can't be phished

You already know a second step at sign-in stops most break-ins. Passkeys and hardware security keys are the best version of that second step — genuinely phishing-resistant, and surprisingly practical to roll out to a handful of employees. This guide explains what they are and how to start.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. I've spent 30+ years helping small businesses with their technology, in plain language. These sound futuristic, but they're easier to use day to day than the codes you may be typing now — often it's just a fingerprint, a face, or a tap.

The whole promise here is simple: with a passkey or a security key, even if an employee is fooled by a perfect fake login page, there's nothing for the crook to steal and reuse. That's a different and much stronger kind of protection than a code you can be tricked into typing.

★ I can set these up for your team in one visit

Rolling out passkeys or security keys to a few staff is a friendly afternoon's work, and I'll make sure everyone has a backup so nobody gets locked out. Call or text me at (330) 200-8042.

The whole guide, on one page

If you remember only these things, you've got the heart of it.

- ❑ **Passkeys and security keys are phishing-resistant** — they're bound to the real website, so a fake page captures nothing reusable.
- ❑ They're **stronger than SMS codes or app codes**, which a clever scam can still trick out of you.
- ❑ A **passkey** lives on a device you already own — your phone or computer; a **security key** is a small physical device you plug in or tap.
- ❑ They're **practical for a handful of staff** — start with your most valuable accounts (admins) first.
- ❑ Give every person a **backup** key or passkey and a **recovery path** so nobody ever gets locked out.
- ❑ They work right in Microsoft 365 and Google Workspace — see our two sign-in guides for the admin side.

! Codes can be phished; keys and passkeys can't

A texted or app code feels secure, but a convincing fake page can still ask you to type it in — and attackers do exactly that. Passkeys and security keys remove that trick entirely, which is why they're the strongest second step you can give your team.

What 'phishing-resistant' actually means

This is the whole reason to bother, so let's make it crystal clear in plain English.

Most scams work by getting you onto a fake login page that looks just like the real one. You type your password; if there's a code, the fake page asks for that too, and quietly passes both to the attacker in real time. The code didn't protect you, because you were tricked into handing it over.

A passkey or security key can't be fooled this way. Behind the scenes it's tied to the **real** website address, and it only answers to that real site. On a fake page it simply does nothing useful — there's no password and no code to capture, and nothing the crook could carry back to the genuine site to log in. That's what 'phishing-resistant' means: the trick that beats codes doesn't work here.

! The lock checks the door, not just the key

An ordinary code is like a key that opens anything shaped like your door — including a fake one. A passkey checks that it's the **real** door before it does anything. That one difference stops the scam that fools everything else.

Passkey or security key? The plain difference

People mix these up constantly. They're cousins — same phishing-resistant idea, different form.

A passkey

A **passkey** lives on a device you already own — your phone, tablet, or computer. You unlock it the way you already unlock that device: a fingerprint, your face, or a PIN. There's nothing extra to carry and often nothing to buy. For most everyday stuff, a passkey on their phone is the easy, free path to phishing-resistant sign-in.

A security key

A **security key** is a small physical device — about the size of a thumb drive — that you plug into a USB port or tap against your phone. It holds the sign-in secret on the device itself. Because it's a separate object you keep on a keychain, it's a strong choice for your most important accounts, like an administrator.

✓ Same protection, choose by fit

Both are phishing-resistant, so you're not choosing between strong and weak — you're choosing what fits. Passkeys for easy everyday use, physical keys for the accounts you want locked down hardest.

Just how strong is this?

You don't have to take my word that keys are better — the numbers are striking.

Google has reported that hardware security keys blocked roughly 100% of automated bot attacks, about 99% of bulk phishing attempts, and around 90% of targeted attacks in its testing. Those are the kinds of attacks that slip past passwords and even past ordinary codes — and the key stopped nearly all of them.

I share those figures the way Google reported them, not as a promise about your exact situation. But the direction is unmistakable: a phishing-resistant key or passkey is a big step up from a texted code, especially against the sophisticated scams that target businesses with money to move.

✓ Strongest where it matters most

If an attacker singled out your business — a convincing email aimed right at your bookkeeper — an ordinary code might not save you, but a key very likely would. That's exactly the scenario these are built for.

Start with the accounts that matter most

You don't have to roll this out to everyone on day one. Begin where the payoff is biggest.

The smart first targets are your most powerful and most exposed accounts: your Microsoft 365 Global Administrator or Google Workspace super-admin, the owner's account, and anyone who can move money or reach sensitive customer data. Those are the accounts an attacker wants most, so they deserve the strongest lock first.

- Admins first — the keys to the kingdom (see our 'Who's the Admin?' guide).
- Then anyone who handles payments, payroll, or banking.
- Then anyone with access to sensitive customer, patient, or donor records.
- Then the rest of the team, as time and budget allow — passkeys make this cheap.

✓ Protect the crown jewels first

If you only equip a few people this quarter, make it the admins and the money-movers. Protecting those accounts first gives you the most safety for the least effort.

The one rule you can't skip: a backup

Stronger sign-in raises one real worry — getting locked out. Here's how you make sure that never happens.

If a person's only passkey is on a phone that's lost, stolen, or dropped in a lake, you don't want them locked out of their work. So the rule is simple and non-negotiable: **every person gets a backup**. That might be a second passkey on another device, a spare security key kept safe, or an alternate sign-in method held in reserve.

Alongside the backup, make sure there's a **recovery path** — a way an admin can help someone regain access if everything goes sideways. This is exactly where a break-glass admin account (from our sign-in guides) earns its keep. Set the safety net up first, then tighten the locks with confidence.

! No backup, no rollout

Never give someone a single passkey or key with no fallback. One lost phone shouldn't be able to lock a person out of their livelihood. A backup per person is the price of doing this right.

What signing in feels like day to day

Here's the pleasant surprise: strong usually means easier, not harder.

With a passkey, signing in often means just unlocking the way you already do — a fingerprint, a glance at your phone, or a quick PIN. No password to remember, no code to wait for and type. With a security key, you plug it in or tap it and maybe touch a little button. Either way it's a second or two.

For a lot of people this is actually **less** hassle than the codes they've been fumbling with — no more squinting at a text message or racing a 30-second timer. Once your team tries it for a few days, the usual reaction is that they wish they'd switched sooner.

✓ Let people feel it before they judge it

If someone's skeptical, set up one account with a passkey and let them sign in a couple of times. The convenience sells itself far better than any explanation I can write here.

Where codes still fit in

None of this means texted and app codes are worthless — it means they're a rung down the ladder.

Any second step is far better than a password alone, so if your team is on app or text codes today, that's real protection worth keeping until you upgrade. The point isn't to panic — it's to know that codes can still be phished, and to move your most valuable accounts to something that can't.

Second step	Phishing-resistant?	Good for
Text (SMS) code	No	Last resort
App prompt/code	No	Everyday baseline
Passkey	Yes	Most staff
Security key	Yes	Admins, high-value

✓ **Upgrade in order of value**

Think of it as a ladder: get everyone at least onto app codes, then lift your admins and money-movers up to keys or passkeys. You don't have to do it all at once to be meaningfully safer.

Two ways to equip your team

Both are phishing-resistant, so the choice is about what suits each person and account — not about settling for less protection.

Passkeys on phones and computers

The easy, low-cost path for most of your everyday staff — nothing extra to buy, nothing extra to carry.

- Uses the fingerprint, face, or PIN people already use to unlock their device.
- Free or nearly free — it lives on hardware they already have.
- Great for everyday team members and anyone who'd rather not carry an extra gadget.
- Keep a backup passkey on a second device so a lost phone isn't a lockout.

Physical security keys

A small device on a keychain — the strongest choice for your most important and most targeted accounts.

- Ideal for admins (Global Admin, super-admin) and anyone who moves money.
- A separate physical object, so it's not tied to one phone's condition.
- Buy a spare for each person who uses one, and store it somewhere safe.
- A good fit where an insurer or a rule wants the strongest demonstrable control.

★ Not sure who needs which?

Tell me how your team is set up and who touches the sensitive stuff, and I'll help you pick passkeys here and physical keys there — and make sure everyone has a backup. Call (330) 200-8042.

A calm way to roll this out

A little planning turns this from a scary tech project into a pleasant afternoon.

- **Pick your first accounts** — admins and money-movers.
- **Decide passkey or key** for each, based on the last page's split.
- **Set up the backup first** — a second passkey or spare key, and a recovery path, for every person.
- **Enroll one person end to end** and have them sign in a few times before you do the rest.
- **Roll out to the group**, with a quick how-to and someone on hand for questions.
- **Write down** who has what and where the backups live.

✓ One person first, then the rest

Proving the whole flow with a single willing person — enroll, back up, sign in, recover — shakes out any surprises before the whole team is waiting on you. It's the difference between a smooth rollout and a stressful one.

They work right in Microsoft 365 and Google Workspace

You don't need special software — the two services most small offices already use support these directly.

Both Microsoft 365 and Google Workspace let you add passkeys and security keys as a sign-in method, and both treat them as a strong form of the second step. The exact menu names and screens move around over time, so check your current admin center or account settings rather than hunting for an exact click that may have been renamed.

Our companion guides, 'Locking Down Microsoft 365 Sign-Ins' and 'Locking Down Google Workspace,' cover the admin side — turning on and enforcing the second step for everyone. This guide is the natural next step: making that second step the strongest kind for the people who need it most.

✓ Settings names change — the capability doesn't

If the enrollment screen doesn't match a guide word for word, don't worry. Look under your account's security or sign-in methods for an option to add a passkey or security key, or call me and I'll find it on your version.

What happens if a key or phone goes missing

This is the question everyone asks, and the answer is reassuring — if you set up the backup.

A lost security key or a stolen phone is far less scary than a stolen password. The key or passkey doesn't carry your other secrets, and a thief who finds it usually can't use it without also unlocking the device or knowing a PIN. Still, you act: remove that lost key or passkey from the account so it can never be used, and the person switches to their backup.

That's the whole reason the backup rule exists. With a spare passkey or key already in place, a lost device is a quick 'remove the old one, use the spare' — an afternoon's inconvenience, not a crisis. Then set up a new backup so you're never down to one again.

! Remove a lost key from the account promptly

Treat a missing key or phone like a missing building key: assume it could fall into the wrong hands, and take it off the account right away. The backup is what lets you do that without locking anyone out.

Why your admins should go first and strongest

If there's one place to spend the extra few dollars on a physical key, it's your administrator accounts.

An administrator account — the Global Admin in Microsoft 365, the super-admin in Google Workspace — can change everything: add and remove people, reach anyone's data, rewrite security. It's the single account an attacker most wants, and the one where a phishing-resistant key pays off most. Our 'Who's the Admin?' guide explains why keeping that power separate and scarce matters.

So put a security key or passkey on every admin account first, give each admin a backup, and keep those keys properly safe. Locking down the keys to the kingdom with a lock that can't be phished is about the highest return any security step offers a small business.

! The most powerful account needs the strongest lock

A Global Admin or super-admin protected only by a password and a code is a tempting target. Of everything in this guide, putting a phishing-resistant key on your admin accounts is the step I'd never skip.

What it costs and how much effort it is

Let's be honest about the real-world price — in dollars and in time.

Passkeys usually cost nothing: they live on phones and computers your team already owns. Physical security keys are inexpensive little devices, and you'll want a spare for each person who uses one. I won't name brands or quote a price here — those change — but they're a modest one-time expense, not a subscription.

The effort is mostly the first setup: picking accounts, enrolling people, and setting up backups. After that, it quietly makes everyone's daily sign-in easier. For a handful of staff it's genuinely an afternoon's project, not a big IT undertaking — which is exactly why it's so practical for a small business.

✓ A one-time cost, a lasting payoff

Unlike a lot of security spending, this isn't a recurring bill. A few keys and an afternoon buy you phishing-resistant sign-in that keeps working, and makes logging in nicer every single day.

The mistakes that trip people up

A few missteps can turn an easy win into a headache. Now you'll avoid them.

- **No backup** — the single biggest mistake; one lost phone becomes a lockout.
- **Starting with everyone** instead of admins and money-movers first.
- **Leaving old weak methods on** — if a texted code still works as a fallback, a scam can aim there instead.
- **Not removing a lost key** from the account promptly.
- **No recovery path** and no break-glass admin to help someone back in.
- **Not writing down** who holds which key and where backups live.

! A weak fallback undoes a strong lock

If you give an admin a phishing-resistant key but leave a text-message code as an easy fallback, a clever attacker will simply target the weaker option. As you strengthen the important accounts, tighten their fallbacks too.

A simple rollout plan

Here's the whole job in a sensible order, biggest wins first.

- ❑ List your accounts in order of value — admins and money-movers at the top.
- ❑ Choose passkey or physical key for each, and buy spares where you'll use keys.
- ❑ Make sure a **break-glass admin** and a recovery path exist before you start.
- ❑ Enroll one admin end to end — primary **and** backup — and sign in a few times.
- ❑ Roll out to the rest of your priority accounts, each with a backup.
- ❑ Write down who has what and where backups live, and tighten weak fallbacks.

Work top to bottom and your most important accounts are phishing-resistant within an afternoon. If the backup-and-recovery part makes you nervous, that's exactly the piece I'm glad to handle with you.

A few words to tell your team

People adopt this happily when you frame it right. Here's the plain-language pitch.

Tell your team three things. First, this makes signing in **easier** — usually just a fingerprint or a tap, no codes to type. Second, it means that even if they get fooled by a fake email, the crooks get nothing they can use — so it takes the pressure off being perfect. Third, everyone has a backup, so nobody's going to get locked out.

That framing — easier, safer, and safe against lockout — turns what could feel like another rule into something people actually like. The technology does the hard part; your job is just to introduce it kindly.

✓ Lead with 'easier,' not 'more secure'

Security pitches make eyes glaze over. 'You won't have to type codes anymore' gets people on board fast — and the security comes along for the ride.

Keeping it tidy over time

A light touch keeps your keys and passkeys working for you as people and devices change.

A couple of times a year, confirm each person still has a working primary and backup, remove keys or passkeys tied to old phones or departed staff, and make sure new hires get set up as part of their onboarding. When someone leaves, remove their keys and passkeys the same day — our offboarding guide folds this right into the departure checklist.

As you add new staff or new systems, keep extending the same habit: the valuable accounts get the strongest second step, everyone gets a backup, and you write down who holds what. It stays simple as long as you keep it current.

✓ Fold it into checks you already do

This review pairs naturally with your admin-account review and your offboarding steps. Handle them together and strong sign-in just becomes part of how your office runs.

The whole idea, in one view

Keep this handy — it's the plan on a single page.

Question	Answer
Strongest second step?	Passkey or security key
Cheapest to start?	Passkeys on phones
Who goes first?	Admins and money-movers
The one rule?	A backup for everyone
If one is lost?	Remove it, use the backup

★ **Want me to set this up for your team?**

I'll pick the right mix of passkeys and keys, enroll everyone with a backup, lock down your admins first, and leave you with a simple written record. Call or text (330) 200-8042.

Common Questions

The questions I hear most from owners about passkeys and security keys.

Q: What's the difference between a passkey and a security key?

A passkey lives on a device you already own — your phone or computer — and you unlock it with a fingerprint, face, or PIN. A security key is a small physical device you plug in or tap. Both are phishing-resistant; passkeys are the easy free path, keys are great for your most important accounts.

Q: Are these really better than the codes I use now?

Yes. Codes can still be phished — a fake page can ask you to type them in. Passkeys and keys are bound to the real site, so a fake page gets nothing reusable. Google has reported hardware keys blocked the vast majority of phishing and targeted attacks in its testing.

Q: What if I lose my phone or my key?

That's exactly why everyone gets a backup — a second passkey or spare key, plus a recovery path. You remove the lost one from the account so it can't be used, switch to the backup, and set up a fresh backup. An inconvenience, not a crisis.

Q: Do I have to give these to my whole team at once?

No. Start with the accounts that matter most — your admins and anyone who moves money or touches sensitive data — then expand as time and budget allow. Passkeys make rolling out to everyone eventually quite cheap.

★ Still have a question?

There's no silly question here. Call or text me at (330) 200-8042 and I'll give you a straight, plain-English answer — and I don't sell any brand of key, so it's just honest advice.

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 rolling out passkeys and security keys for your staff 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

Why a Fake Page Fails

Codes can be stolen; keys can't

	Password + code	Passkey or key
On a fake page	You can type it	Does nothing
What crook gets	A reusable code	Nothing usable
Bound to real site	No	Yes
Beats live phishing	No	Yes

Phishing-resistant means the trick that beats codes doesn't work.

Passkey vs. Security Key

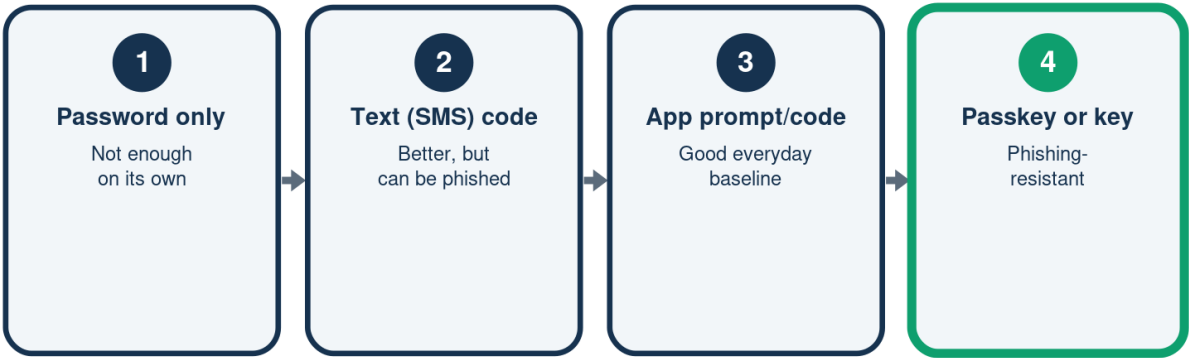
Same protection, different form

	Passkey	Security key
Lives on	Phone/computer	Small device
You unlock with	Fingerprint/face	Plug in or tap
Cost	Usually free	Inexpensive
Best for	Most staff	Admins

Passkeys for easy everyday use; keys for your crown-jewel accounts.

The Second-Step Ladder

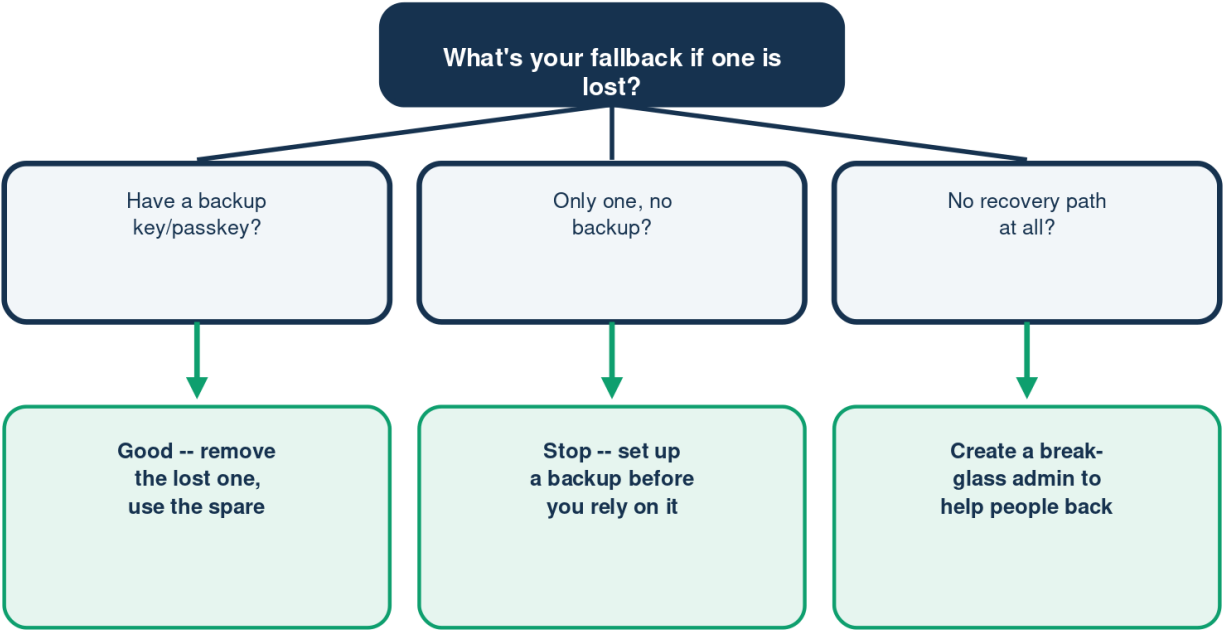
Any step up is real protection



Lift your admins and money-movers to the top rung first.

Worried About Lockout?

The backup rule is what makes this safe



No backup, no rollout -- one lost phone must never mean a lockout.

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