

How to Enroll in Passkey Authentication

A Step-by-Step Guide by IT Support RI

A plain-English walkthrough for setting up a **passkey** on your Microsoft 365 business account — a faster, phishing-proof way to sign in.

The most secure way to sign in. A passkey lets you approve sign-ins with your phone instead of a password or a code. This guide makes setting one up quick and painless — about five minutes, start to finish.

SECURITY

Phishing-proof

TIME NEEDED

About 5 min

DIFFICULTY

Easy

THE BASICS

What a passkey is, in plain English

A passkey is a digital key kept safely on your phone. Instead of typing a password or a code, you approve sign-ins with your **fingerprint, face, or PIN**. It can't be phished, guessed, or reused — which is exactly why it's the most secure way into your Microsoft 365 account. Setting one up takes about five minutes.

What you'll need

- Your smartphone (iPhone or Android)
- Your work email address & password
- A screen lock (fingerprint, face, or PIN)
- About 5 quiet minutes

What's a passkey?

Think of it as a digital key kept safely on your phone. Instead of typing a password or code, you confirm with your **fingerprint, face, or PIN**. It can't be phished, guessed, or reused — which is exactly what makes it so secure.

Not sure if this applies to you? It's the Microsoft account behind your business email, Outlook, Teams, and Office. Runs on Google Workspace instead? See page 5. Unsure? Just call us — our number is on the last page.

THE BASICS

Why a passkey — and how it works

You didn't start your business to become a security expert. Here's what makes a passkey different, in about a minute.

PASSWORDS & CODES

The usual way to sign in

- ✗ Passwords can be guessed, reused, or leaked in a breach.
- ✗ Codes you type can be intercepted or phished on a fake page.
- ✗ It's one more thing to remember, wait for, and type in.

A PASSKEY

The simpler, safer way

- ✓ You approve sign-in with fingerprint, face, or PIN.
- ✓ Nothing to type, so there's no code for anyone to steal.
- ✓ It only works on the real Microsoft site — phishing pages fail.
- ✓ Faster every single day, on every device you set up.

Safe by design

Why a passkey can't be phished. Your passkey never leaves your phone, and it only works on the genuine Microsoft sign-in page. There's no code to intercept and nothing to type into a fake site — so the tricks scammers rely on simply don't work. That's what makes a passkey the strongest way to protect your Microsoft 365 account.

BEFORE YOU BEGIN

A quick readiness check

Run through these once — if any box is a "no," the fix is simple, or just give us a call.

- | | |
|---|--|
|  A supported phone
iPhone on iOS 16 or newer, or Android 9 or newer.
Most phones from the last several years qualify. |  A screen lock turned on
Fingerprint, face unlock, or a PIN. This is what keeps your passkey protected — it's required. |
|  Your current sign-in handy
You'll verify once with your existing method (your password, an app prompt, or a code) to get started. |  Five uninterrupted minutes
Do it at your desk or anywhere you can use your phone. You only set it up once per device. |

 **Tip:** Rather not do this yourself? That's exactly what we're here for — we can set it up for you or your whole team. See the last page.

 Set it up on your phone

The simplest way — you'll only need your phone

This works for most people and takes about five minutes. Prefer to start from a computer? See page 4.

1 Install Microsoft Authenticator
On your phone, open the **App Store** (iPhone) or **Google Play** (Android), search **Microsoft Authenticator**, and install it. Check the publisher reads "Microsoft Corporation."

2 Add your work account
Open the app. If your work account isn't listed, tap , choose the **work account** option, and sign in with your work email and password.

3 Confirm it's really you
You may be asked to verify once with your current method — approve a prompt, enter a code, or use your password. This just confirms it's really you.

4 Tap "Create a passkey"
In the app, tap your account, then tap **Create a passkey**. If it asks you to set up a screen lock first, follow the prompt to add one — it's required.

5 Turn on Authenticator as your passkey app
The app guides you to a quick setting — switch it on:

iPhone: Settings → General → AutoFill & Passwords → turn on **AutoFill Passwords and Passkeys** and check **Authenticator**.

Android: Settings → Passwords, passkeys & accounts → set **Authenticator** as a passkey provider.

6 Finish up
Return to the Authenticator app and tap **Done**. You'll now see **Passkey** listed on your account. Tap **Done** once more.

 **That's it — you're done!** Next time you sign in to Microsoft 365, just approve it with your fingerprint, face, or PIN — nothing to type.

Microsoft 365 · from a computer

Prefer to start on your computer?

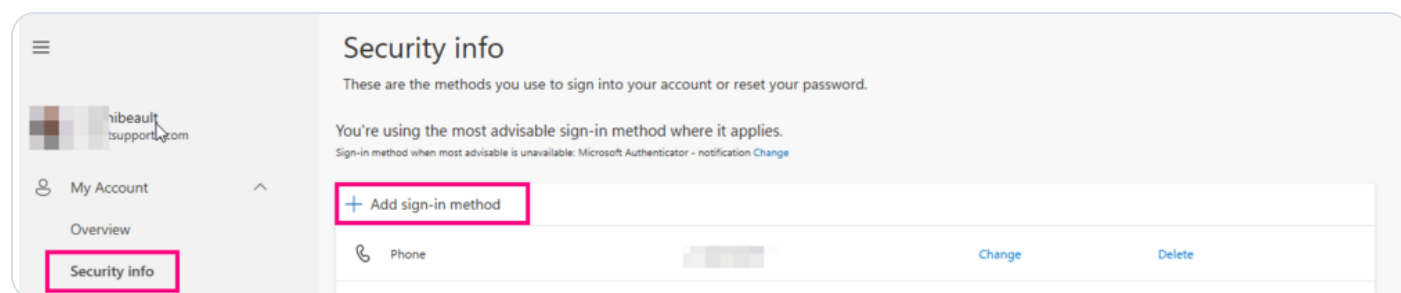
You'll still finish on your phone, but you can kick things off from a web browser — handy when you're at your desk.

- 1 **Go to your security page**
Open a web browser and go to aka.ms/mysecurityinfo. Sign in with your work email and password.
- 2 **Add a new sign-in method**
Click **+ Add sign-in method**, then choose **Paskey in Microsoft Authenticator**.
- 3 **Follow the on-screen guide**
The website walks you through it and asks you to open the Authenticator app on your phone to create the passkey there — the same phone steps from page 3. No app yet? It'll help you install it.
- 4 **Finish on your computer**
Once the app confirms the passkey, return to your computer, click **Next**, then **Done**. Your new passkey appears in the list.

Stuck on a step? Click "Having trouble" → "create your passkey a different way," or just call us.



One requirement for computers: Signing in on a workstation with the passkey in Microsoft Authenticator uses a quick **Bluetooth** handshake between your phone and the computer to confirm they're close together — so the computer needs Bluetooth turned on. (Not required if the passkey is saved on the computer itself or you use a security key.)



Step 2 — Add sign-in method

OPTIONAL · ADVANCED

Using a hardware security key?

Using a physical FIDO2 key (like a YubiKey)? Choose **Paskey** at step 2 and set its PIN when prompted.

ONE LAST THING

Give it a quick test

Sign out and back in once to confirm your new passkey works. **Any trouble, we're one call away.**

 Google Workspace (Gmail)

Runs on Google instead? Do this.

Passkeys work on Google Workspace too — same idea, same security benefits. Here's the short version.

- 1 Open your Google security settings**
On a computer, go to myaccount.google.com → **Security**. Under "How you sign in to Google," open **2-Step Verification** (turn it on if it isn't already).
- 2 Best option — add a passkey**
Open **Passkeys and security keys** → **Create a passkey**, then confirm with your fingerprint, face, or device PIN.
- 3 Or — use an authenticator app**
Find **Authenticator** → **Set up authenticator** → scan the QR code with Google or Microsoft Authenticator → enter the 6-digit code.
- 4 Give it a quick test**
Sign out and back in once to confirm your new passkey works. That's all there is to it.

Rolling this out to your whole team?

We can enable passkeys across your organization and guide every employee through enrollment, so your whole team is on fast, phishing-proof sign-in. One less thing on your plate.

 **401-522-5200** **Set it up on two devices**

We recommend enrolling a passkey on more than one device (say, your phone and your laptop). If you ever lose one, you can still sign in with the other — no lockout.

 You'll still have your password

A passkey is an additional, phishing-proof way to sign in. Keep your password too — Microsoft still accepts it alongside your new passkey whenever you need it.

THE QUESTIONS WE HEAR MOST

Quick answers

Q Why should I set up a passkey?

It's the fastest and most secure way to sign in to Microsoft 365. There's no code to type and nothing to remember, and it can't be phished or stolen the way a password or typed code can.

Q Is a passkey safe? What if I lose my phone?

Very — a passkey can't be phished or intercepted, and it never leaves your device. If you get a new phone, just set up the app again on the new device and create a fresh passkey. We can help remove the old one.

Q The app is asking me to set a screen lock.

That's normal and required — it's what keeps your passkey protected. Add a fingerprint, face unlock, or PIN on your phone, then continue where you left off.

Q I don't see "Create a passkey."

Your account may need a setting switched on from our side. Give us a quick call and we'll enable it while you're on the line.

Q What makes a passkey more secure?

It never leaves your device, and it only works on the genuine Microsoft sign-in page. So there's no code for anyone to intercept, and fake phishing pages simply don't work against it.

Q Can you just do it for me?

Absolutely. If you'd rather not do this yourself, that's what we're here for — reach out and we'll take care of it for you or your whole team.

Rather we just handle it?

We can set this up for you or your entire team, start to finish.
No question is too small.

Or reply to the email this guide came with, and we'll follow up.

 **401-522-5200**