CHECKLIST · SCAMS & SECURITY

Passkeys explained for small business: what they replace, where they work and where they don't

Published 30 September 2026. Read the full story, sources and any updates at digitaladvisors.com.au/journal/passkeys-small-business-explained/

- [ ] **Create a passkey for your main email account.** Open your Google or Microsoft account security settings and add a passkey, on a phone or computer with Android 9 or later, iOS 16 or later, Windows 10 or later or macOS Ventura or later.
- [ ] **Keep a second sign-in method on that account.** Leave an authenticator app or backup option in place until you've signed in with the passkey on more than one device.
- [ ] **Ask your IT provider or Workspace or Microsoft 365 administrator whether passkeys are allowed for staff.** Google says Workspace users may not be able to sign in with only a passkey, and Microsoft Entra lets administrators choose which passkey types are permitted.
- [ ] **Check where each passkey is stored.** For each business-critical account, record whether its passkey is in iCloud Keychain, Google Password Manager, Microsoft Password Manager or a hardware security key, and name the person whose device or account unlocks it.
- [ ] **Buy or nominate a hardware security key for owners and administrators (our suggestion).** Google lists FIDO2 hardware keys as supported, and Microsoft Entra supports them as device-bound passkeys.
- [ ] **Write down the lost-phone steps.** Sign in from another device and remove the lost device's passkey (Google's stated step), then confirm the account's recovery phone number and recovery email are current.
- [ ] **Turn on two-factor authentication where a service has no passkeys.** Set up an authenticator app on each account that has no passkey option.

General information only, not legal, tax or financial advice. Check the full story and its sources before acting.

- [ ] **Protect the account that syncs your passkeys.** Apple says iCloud Keychain needs two-factor authentication on the Apple Account. Confirm 2-Step Verification (Google) or two-step verification (Microsoft) is on, and that the recovery phone number and email are current, for the account that holds your synced passkeys.

NOTES

General information only, not legal, tax or financial advice. Check the full story and its sources before acting.