

Turning on two-step sign-in

Easy · 5 min per account · Free

Two-step sign-in (also called two-factor or multifactor authentication) means a stolen password alone can't open your account. Turn it on for your most sensitive accounts first: bank, credit cards, email, social media, tax site and payment apps. Choose a passkey, security key or authenticator app over text codes when offered, because text codes can be stolen with a SIM swap. Save the backup codes somewhere safe, and never give a code to anyone who contacts you.

YOU'LL NEED

- ☐ Your phone
- ☐ A safe place for backup codes
- ☐ Your account logins (ideally in a password manager)

WHAT TO KNOW

- 1 **Open the account's settings, then its security section.** It may be called Security, or Password and Security.
- 2 **Look for two-factor authentication, two-step verification or multifactor authentication.** It usually isn't on by default.
- 3 **Pick the strongest method offered.** Security keys are strongest, because there's no code to steal. Authenticator apps like Google Authenticator, Microsoft Authenticator or Duo are safer than text or email codes. If a site offers a passkey, take it.
- 4 **Save your backup codes.** They let you sign in if you lose your phone or change your number. Each works once, and you can print them and keep them with your passport or other important papers.
- 5 **Start with your most sensitive accounts: bank, credit cards, email, social media, tax filing site and payment apps.** Then add shopping sites. Don't skip email: in CISA's example, a hacked email let scammers into a bank account and other linked accounts.
- 6 **Let it remember only your own devices, never a library or other public computer.**

Watch out Never share a verification code with someone if you didn't contact them first, no matter the story. Getting a flood of login approval requests you didn't start? That's "push bombing," meant to get you to tap approve by accident. Deny them and change your password.

DAD NOTE *Two locks on the front door. Takes a minute, and it's worth it.*

Full lesson: aptkeys.com/tools/passwords-and-sign-in/turning-on-two-step-sign-in/

Checked October 2, 2026. Sources: Federal Trade Commission; Cybersecurity and Infrastructure Security Agency; National Cybersecurity Alliance; Google.