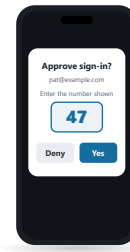


Turn On Two-Factor Microsoft · Google

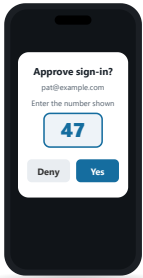
A second step after your password, so a stolen password isn't enough to get into your account.



*We Make
I.T.
Happen!*

1 Why Turn It On?

Even if a scammer **steals your password**, they can't sign in without your phone.



2 Pick Your Second Step

Best: a passkey or an **authenticator app**. **Okay:** a text message code.



3 Microsoft: Security

Go to account.microsoft.com → **Security** → **Manage how I sign in**.



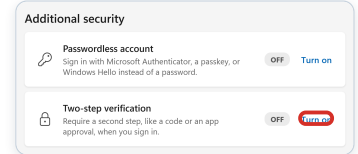
Manage how I sign in

Add ways to prove who you are, and turn on two-step verification.

[Manage how I sign in](#)

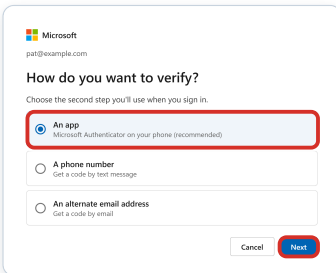
4 Two-Step: Turn On

Under **Additional security**, next to **Two-step verification**, click **Turn on**.



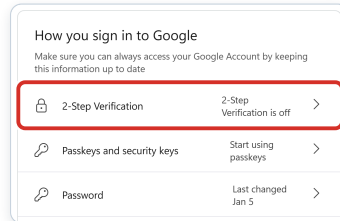
5 Follow the Steps

Choose how you'll verify. The **Microsoft Authenticator** app is best.



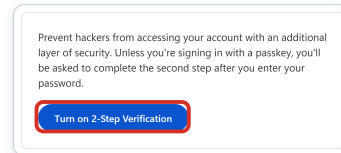
6 Google: Security

myaccount.google.com → **Security & sign-in** → **2-Step Verification**.



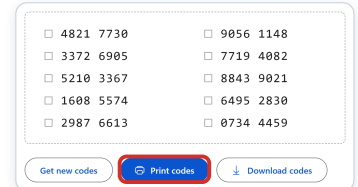
7 Turn On 2-Step

Click **Turn on 2-Step Verification** and follow the prompts to add your phone.



8 Save Backup Codes

Get your **backup codes** (Google) and **recovery code** (Microsoft). Print them.



Keep them on paper, somewhere safe.



Good to Know

- **Never share a code.** No real company will ask you to read it to them. Anyone who asks is a scammer.
- Got a sign-in prompt you didn't expect? **Deny it** and change your password.
- **Businesses:** require MFA for everyone on Microsoft 365. We can set it up for your whole office.



Need Help?

Contact Naples Computers
239-513-1960
We Make I.T. Happen!