

NAPLES COMPUTERS HOW-TO • SECURITY & SAFETY

How to Turn On Two-Factor Authentication

Two-factor authentication (also called 2FA, two-step verification, 2-Step Verification or MFA) adds a second step to signing in, like an approval on your phone. Even if someone steals your password, they can't get in without it. This guide shows how to turn it on for a Microsoft account (account.microsoft.com) and a Google Account (myaccount.google.com), and how to save your recovery and backup codes. Screens are simplified; the labels match Microsoft's and Google's pages as of September 2026.

What is two-factor authentication?

Also called 2FA, two-step verification, or multi-factor authentication (MFA).

1. Your password

Something you know. On its own, it can be guessed, stolen, or leaked.

2. A second step

Something you have: an approval on your phone, a code, or a passkey.

Stolen password? Still safe.

Without your phone, a scammer can't sign in. Microsoft says it blocks over 99% of account attacks.

Which second step is best?

- ☐ **Best: a passkey**
Sign in with your face, fingerprint or PIN. The strongest protection against fake login pages.
- ☐ **Great: an authenticator app**
Microsoft Authenticator or Google Authenticator: tap to approve, or type a 6-digit code
- ☐ **Okay: a text message code**
Much better than nothing, but texts can be intercepted. Microsoft is phasing it out for personal accounts.

Step by step

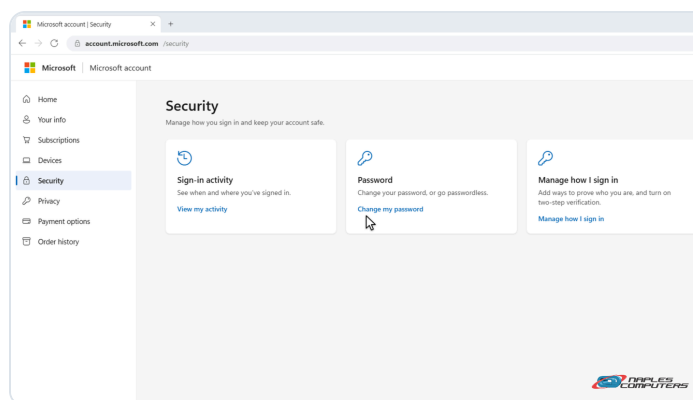
MICROSOFT ACCOUNT

1 Microsoft: go to Security → Manage how I sign in

In your web browser, go to account.microsoft.com and sign in. Click Security.

WHAT TO DO

Choose Manage how I sign in.



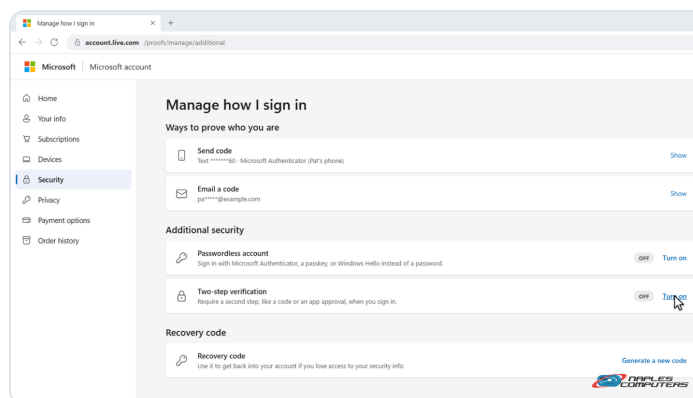
MICROSOFT ACCOUNT

2 Microsoft: Two-step verification → Turn on

Under Additional security, find Two-step verification and click Turn on. Follow the steps and choose how you'll verify: the Microsoft Authenticator app is the best choice.

WHAT TO DO

When it says two-step verification is turned on, you're protected.



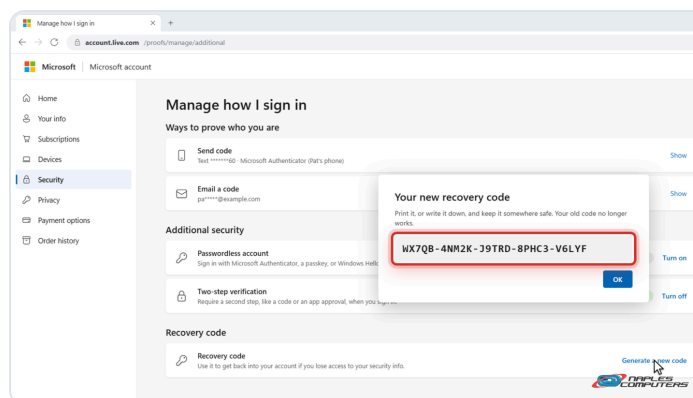
MICROSOFT ACCOUNT

3 Microsoft: save a recovery code

Back on the Manage how I sign in page, under Recovery code, click Generate a new code.

WHAT TO DO

Print it or write it down, and keep it somewhere safe, not on your computer.



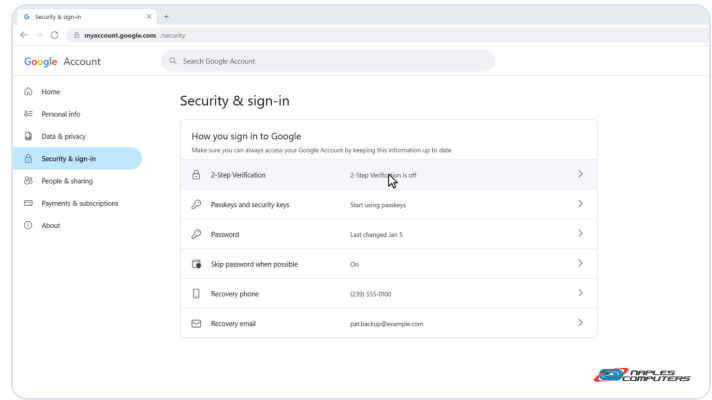
GOOGLE ACCOUNT

4 Google: Security & sign-in → 2-Step Verification

Go to myaccount.google.com and sign in. Click Security & sign-in.

WHAT TO DO

Under “How you sign in to Google”, click 2-Step Verification.



naplescomputers.com

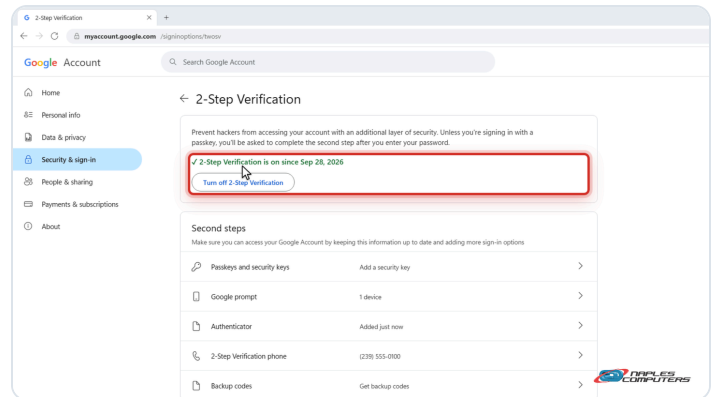
GOOGLE ACCOUNT

5 Google: Turn on 2-Step Verification

Click Turn on 2-Step Verification, and follow the prompts to add your phone or the Google Authenticator app.

WHAT TO DO

Look for “2-Step Verification is on”.



naplescomputers.com

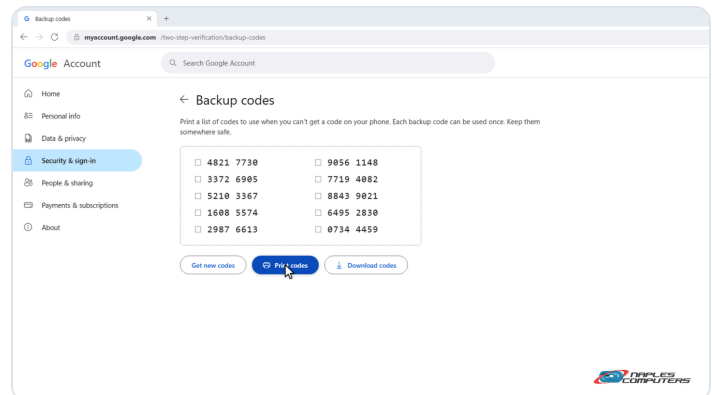
GOOGLE ACCOUNT

6 Google: get your backup codes

On the same page, under Second steps, click Backup codes and get your codes. Each one works once.

WHAT TO DO

Print them or write them down, and keep them somewhere safe.



naplescomputers.com

Never share a code

- ☐ No real company will ask you for your code
Not Microsoft, not Google, not your bank. Anyone who asks is a scammer.
- ☐ Got a prompt you didn't expect? Deny it.
Someone may have your password. Change it right away.
- ☐ Keep backup codes on paper, not on your computer
Somewhere safe, like with your important papers

For businesses: require MFA

- ☐ Turn on MFA for everyone in Microsoft 365
Security defaults or Conditional Access, including the owner and admin accounts
- ☐ Use the Microsoft Authenticator app
With number matching, so a stray prompt can't be approved by accident
- ☐ We can set it up for your whole office
Naples Computers: 239-513-1960

Recap: turn on 2FA

- ☐ Microsoft: Security → Manage how I sign in → Turn on
- ☐ Google: Security & sign-in → 2-Step Verification
- ☐ Use a passkey or an authenticator app
- ☐ Save your backup codes, and never share a code

Start with your email account: whoever controls your email can reset almost every other password. Never share a verification code with anyone who calls or texts you. Setting up MFA for your office? We can do it for you.



Want help turning on two-factor authentication at home or for your office?

Call 239-513-1960

naplescomputers.com · **We Make I.T. Happen!**