

# Instructions for enabling and using 2-Step Verification on your Google account

## How do I turn on 2-Step Verification?

When you enable 2-Step Verification (also known as two-factor authentication, 2FA, or MFA), you add an extra layer of security to your account. You sign in with something you **know** (your password) and something you **have** (like a code sent to your phone).

To set up 2-Step Verification:

1. Go to your Google Account's [2-Step Verification page](#). You will be prompted to sign in to your ULUSD Google Account.
2. Click Get started.
3. Follow the quick step-by-step setup process to use your phone, or select "Show more options" to select an alternate method.

## How do I sign in with 2-Step Verification?

Signing in with 2-Step Verification is easy.

- Go to the sign-in page of your mail or any other ULUSD Google application that employs Google Single Sign-On, and enter your username and password like you normally do.
- Every 30 days (or every time you try logging in on a new device), you'll be sent a push notification to your phone, asked for a six-digit code (also sent to your phone), or prompted to insert a backup code, depending on which option you chose during initial setup. If you want, when you enter your verification, you can choose to trust your computer --

this means you won't be asked for a code again when you sign in from this computer. If you sign in from another computer, however, you'll be asked for your 2nd form of verification.

# Alternate Methods

## What if I don't want to use my phone?

Don't want to use your phone? No problem. You can sign in using [backup codes \(instructions\)](#).

---

Revision #1

Created 2025-07-14 19:01:42 UTC by Blaze King

Updated 2025-07-14 19:01:50 UTC by Blaze King