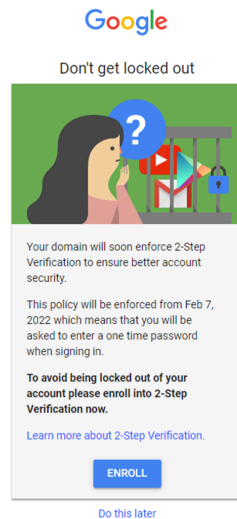


Google 2-Step Verification Guide

Upon your first attempted Google login, you will be prompted to complete a series of steps to enroll in 2-Step Verification. Please note that you **WILL NOT** be prompted to enroll on a Chromebook when logging in to your Google Account via a web browser.

1. Access the 2-step verification setup by [clicking here](https://tinyurl.com/pobgooglemfa). (tinyurl.com/pobgooglemfa)
 - a. You may also be prompted to enroll with the following screen in your web browser. Click “Enroll.”

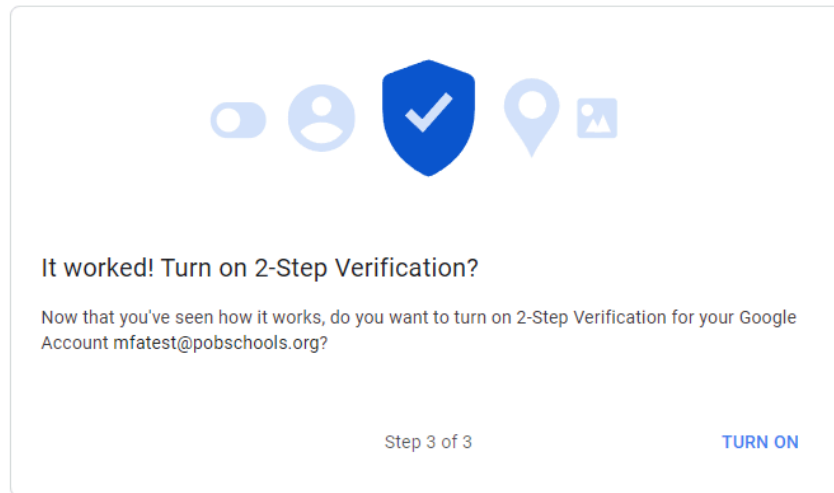


2. Enter a phone number and choose the method you prefer, text or phone call, then click “**Next**.” Google will text or call you with a code. Enter that code when prompted and click “**Next**”
 - a. If you’ve been using your phone with your google account, chances are it’s already paired for usage as two step authentication and you will not be prompted to enter a phone number.

← 2-Step Verification

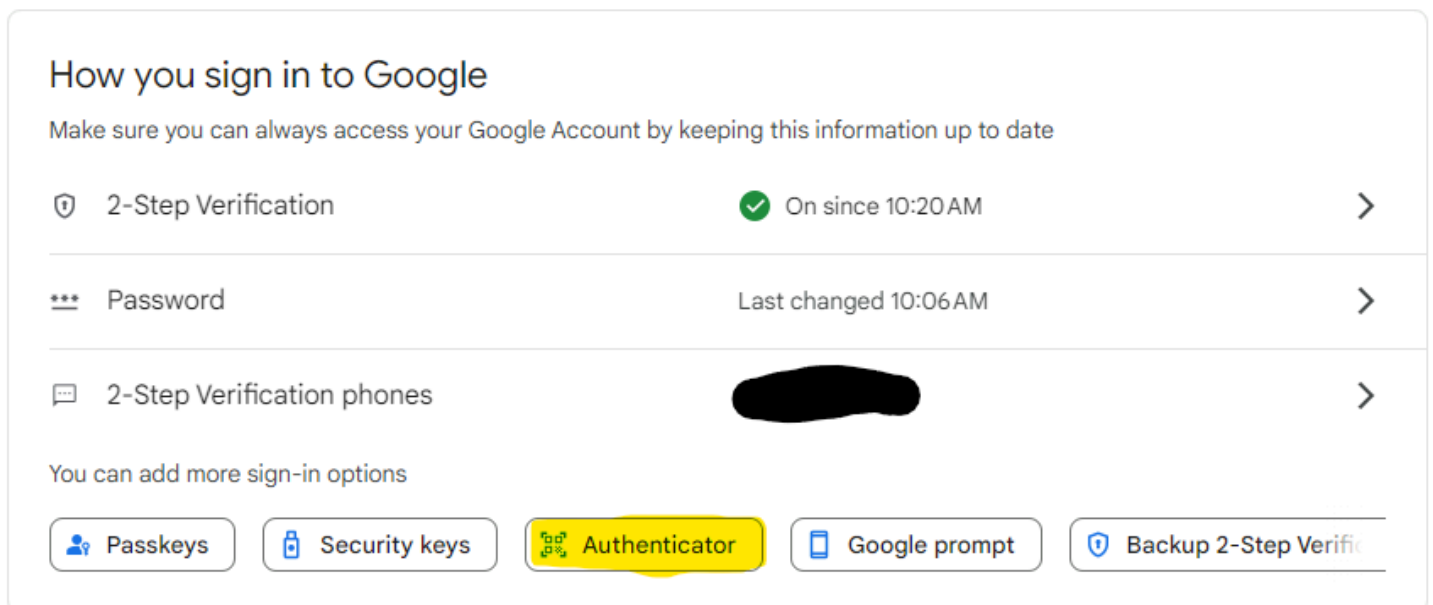
A screenshot of the Google 2-Step Verification setup screen for a phone. At the top, there is a header "← 2-Step Verification". Below the header, there is a row of icons: a lock, a person, a smartphone, a phone, and a key. The main content area is titled "Let's set up your phone". Below the title, there is a question "What phone number do you want to use?". There is a dropdown menu for the country code, currently showing the US flag. Below the dropdown, there is a text input field. Below the input field, there is a note: "Google will only use this number for account security. Don't use a Google Voice number. Message and data rates may apply." Below the note, there is a question "How do you want to get codes?". There are two radio buttons: "Text message" (selected) and "Phone call". Below the radio buttons, there is a link "Show more options". At the bottom, there is a progress indicator "Step 1 of 3" and a "NEXT" button.

3. Click **“Turn On.”**



You'll be brought back to the authentication settings screen and shown all the ways you are able to authenticate into your Google account. **You should add an additional authentication method in addition to text messages.**

4. On the authentication settings screen, **scroll down** to the **“How you sign in to Google Section”** and click the **“Authenticator”** button under the “You can add more sign-in options” text.



5. Click “**Set up authenticator.**”

← Authenticator app

Instead of waiting for text messages, get verification codes from an authenticator app. It works even if your phone is offline.

First, download Google Authenticator from the [Google Play Store](#) or the [iOS App Store](#).



[+ Set up authenticator](#)

6. A QR code will appear on your desktop/chromebook screen. Scan this QR code with your Microsoft Authenticator App (On your mobile device: Launch Microsoft Authenticator app → click the + or three dots in the top right → Add Account → Choose “Other account (Google, Facebook, etc.)” → Choose “Scan QR Code”)
7. Click “**Next**” on your Computer/Chromebook after scanning the QR code.
8. The setup screen on your Computer/Chromebook will prompt you for the 6 digit code that appears on your phone in the Authenticator App. Enter the code and click “**Verify**”.

Set up authenticator app

Enter the 6-digit code you see in the app

[Back](#)

[Cancel](#) [Verify](#)

Remember, authenticator codes are valid for a short period of time, usually 30 seconds or less. If your code fails you may need to grab a new one. Your authenticator app will automatically reset it and give you another for use.

Additional Recommendation: We recommend you enable iCloud/Cloud backup of your MFA accounts in the Microsoft Authenticator app. This will allow you to restore your saved MFA accounts if your phone is lost/stolen/replaced. Instructions on enabling this can be found [here](#).