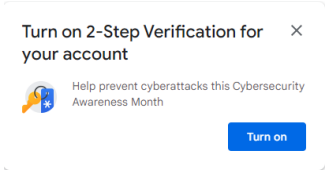
MFA Setup for Staff

MFA is a technology safeguard to protect accounts from unauthorized access. Some other names for MFA are two-factor authentication (2FA) or 2-step verification (2SV). You may already be using this technology with your bank, insurance company, or other online services. One common implementation of MFA is to log-in with a username and password along with a text message code to authenticate access. You can enable MFA on your account at any time. Once we have fully deployed MFA, you will not be able to login until you have MFA enabled on your account. See below for instructions on configuring your accounts to use MFA. Once you have signed on with MFA enabled, you may be periodically prompted to re-verify access. MFA re-verification is infrequent and not required daily.

Allow 2-Step Verification

1. Open your Google Account https://myaccount.google.com/.

2. You may see 

select **"Turn on"**, if not, in the navigation panel on the left, select **"Security"**.

3. Under **"Signing in to Google"** select **"2-Step Verification"** or just click 

4. Follow the on-screen steps.

After you turn on 2-Step Verification, you must complete a second step to verify it's you when you sign in. To help protect your account, Google will ask that you complete a specific second step.

Use Google Prompts

We recommend you sign in with Google prompts. It's easier to tap a prompt than enter a verification code. Prompts can also help protect against SIM swap and other phone number-based hacks.

Google prompts are push notifications you'll receive on:

- Android phones that are signed in to your Google Account.

iPhones with the Smart Lock app , the Gmail app , the Google Photos app , the YouTube app , or Google app signed in to your Google Account.
Based on the device and location info in the notification, you can:

- Allow the sign in if you requested it by tapping **Yes**
- Block the sign-in if you didn't request it by tapping **No**

For added security, Google may ask you for your PIN or other confirmation.

Google Multi-factor Authentication Setup Using Text Messages

Go to https://myaccount.google.com, you may be prompted to sign-in with your WGmail account

Click Security > 2-Step Verification

Click Get Started and sign in with your WGmail account

If you see a prompt to use your phone for Google prompts, click Continue.

Enter your cell phone number, select Text message, and click Send

If you see an error message, click Send again. You may need to click Send multiple times until you see a prompt to “Confirm that it works.”

Enter the code that was texted to your cell phone and click Next.

Click Turn On

Good job! Your WGmail Google account is now secured with 2-Step Verification!

Other Google 2-Step Verification options:

Get verification codes with Google Authenticator

PLEASE NOTE: Skip a second step on trusted devices

If you don't want to provide a second verification step each time you sign in on your computer or phone, check the box next to "**Don't ask again on this computer**" or "**Don't ask again on this device**."

Important: Only check this box on devices you regularly use and don't share with anyone else.