COLORADO
Governor's Office of
Information Technology

Two-factor Authentication for Counties FAQ

This FAQ is a living document and will continue to be updated as needed.

General Information

What is two-factor authentication?

Two-factor authentication (2FA) increases security for the systems it has been applied to by reducing the risk of unauthorized access. It protects the people who have data in the system by allowing only those with legitimate business purposes to access the data, preventing criminals from using it for fraudulent purposes.

2FA requires the additional login step of entering a passcode along with a username and password making it much more difficult for someone with bad intent to obtain login information and access the data of the clients you serve.

Two-factor authentication is also referred to as 2-Step Verification by Google.

When will 2FA be required for county workers?

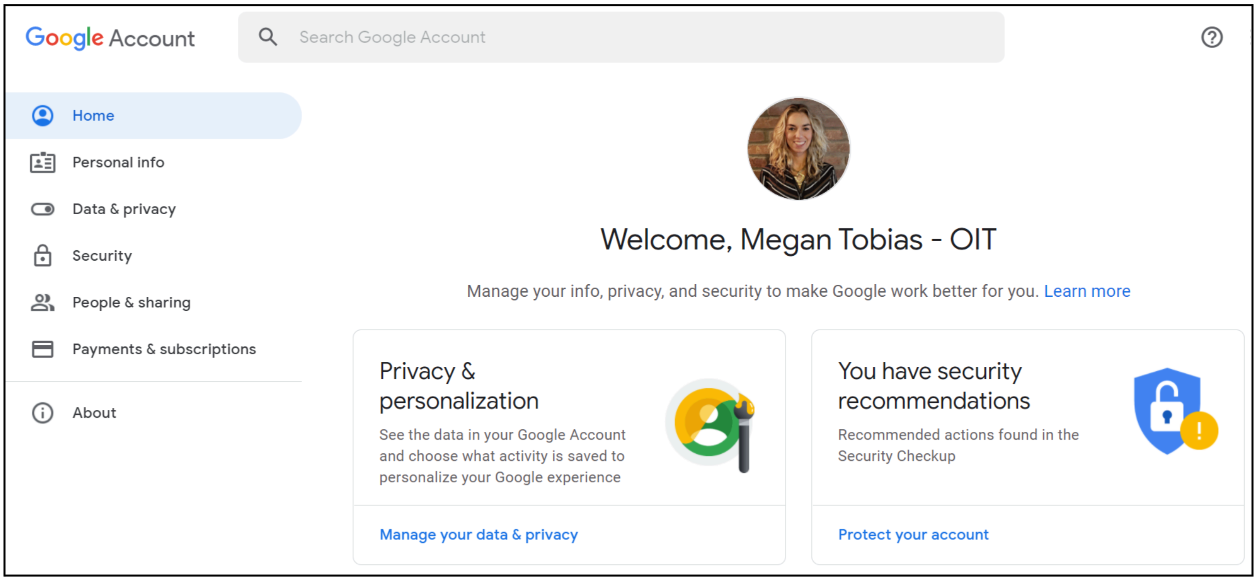
All county users can set up 2FA now. Click this link to get started. You will be directed to Google's page to begin the process for enrolling in 2FA for your Gmail account. Two-factor authentication will be enforced starting January 31, 2022.

Setting Up 2FA

How can I set up 2FA now?

Step 1

Start by heading to myaccount.google.com. You can get there by going to your **Google account**, clicking your photo in the top right-hand corner and selecting **Manage your Google account**.



Welcome, Megan Tobias - OIT

Manage your info, privacy, and security to make Google work better for you. Learn more

Privacy & personalization

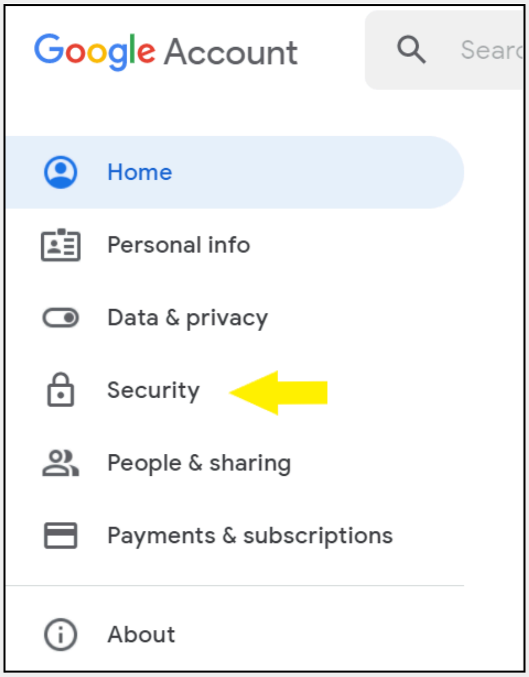
See the data in your Google Account and choose what activity is saved to personalize your Google experience

You have security recommendations

Recommended actions found in the Security Checkup

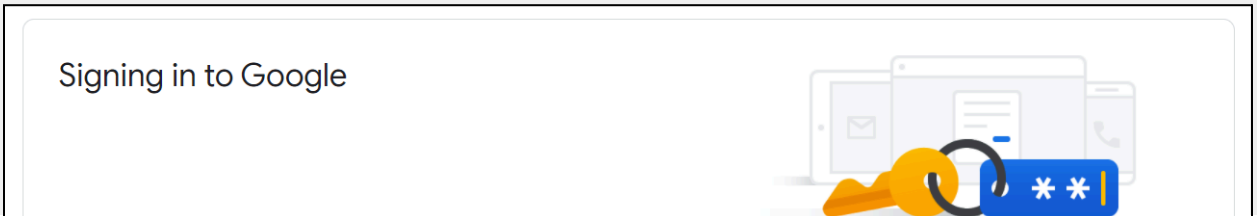
Step 2

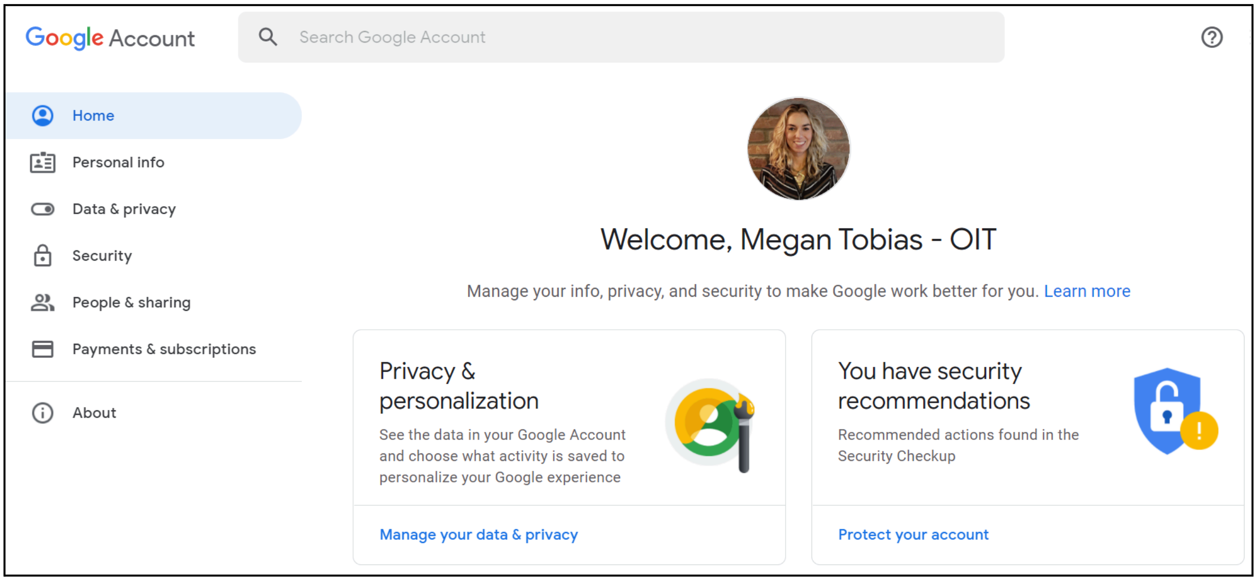
Click on the **Security** tab on the left-hand side in the menu.



Step 3

In the **Signing in to Google** section, click **2-Step Verification.**





Welcome, Megan Tobias - OIT

Manage your info, privacy, and security to make Google work better for you. Learn more

Privacy & personalization

See the data in your Google Account and choose what activity is saved to personalize your Google experience

Manage your data & privacy

You have security recommendations

Recommended actions found in the Security Checkup

Protect your account

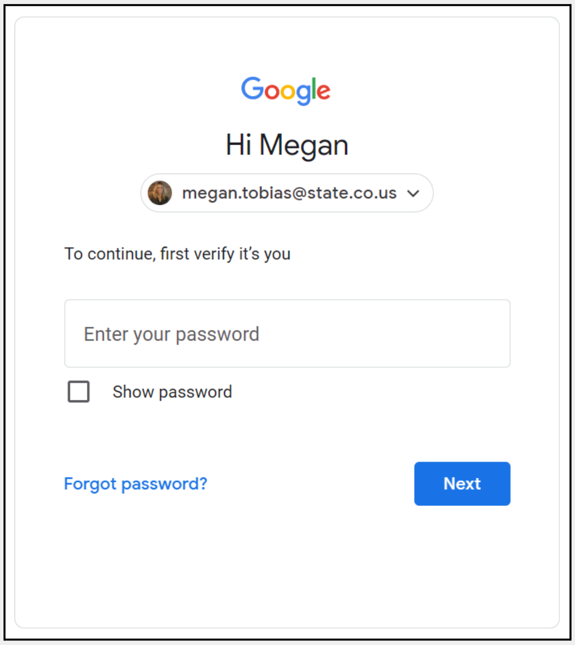
Step 4

Enter your password to confirm it's you and hit **Get Started** on the next page where Google explains 2-Step Verification.

This next page will also show you what devices you'll be able to use to sign in. These are devices Google has deemed secure based on your login history. If the list looks right, click **Continue**.

Verify your current phone number as a backup option then enter the passcode sent to you in order to verify that number.

Lastly, hit **Turn On** and 2FA will be set up.



Hi Megan

megan.tobias@state.co.us

To continue, first verify it's you

Enter your password

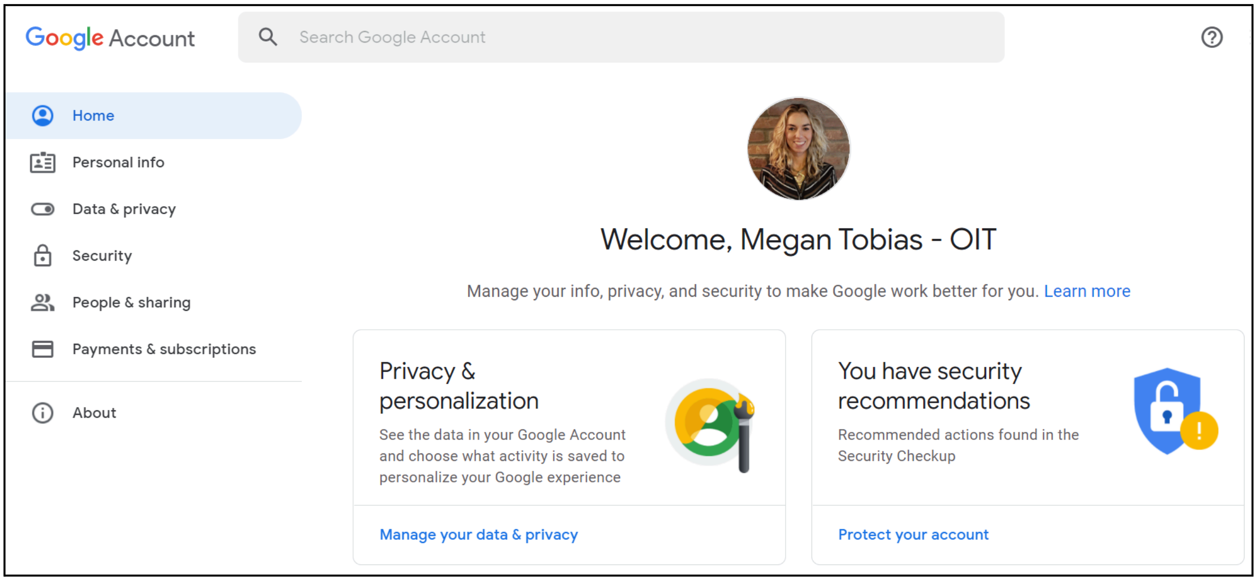
□ Show password

Step 5

After you turn on 2FA, you'll need to complete a second step of entering a passcode to verify it's you when you sign in. You will have several choices as to how you receive that code.

What if I'm not able to set up 2FA for my Google account?

Contact the OIT Service Desk: Call 303.239.HELP, Online at OIT Customer Service Portal or email.



Welcome, Megan Tobias - OIT

Manage your info, privacy, and security to make Google work better for you. Learn more

Privacy & personalization

See the data in your Google Account and choose what activity is saved to personalize your Google experience

You have security recommendations

Recommended actions found in the Security Checkup

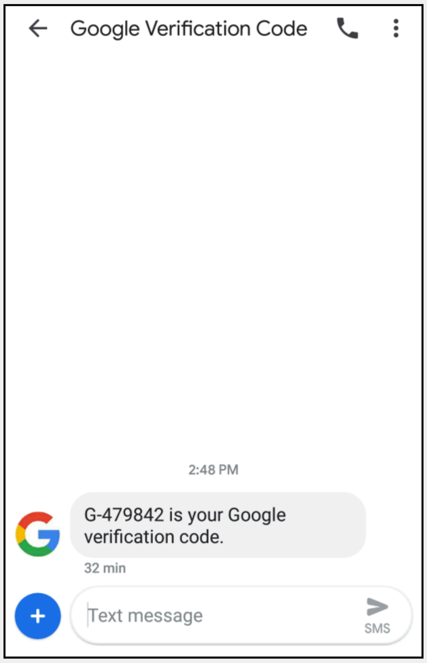
Passcodes

How will I receive my passcode?

When you set up 2FA, you will have several choices on how you can receive your passcode.

Option 1: Use a verification code from a text message or call.

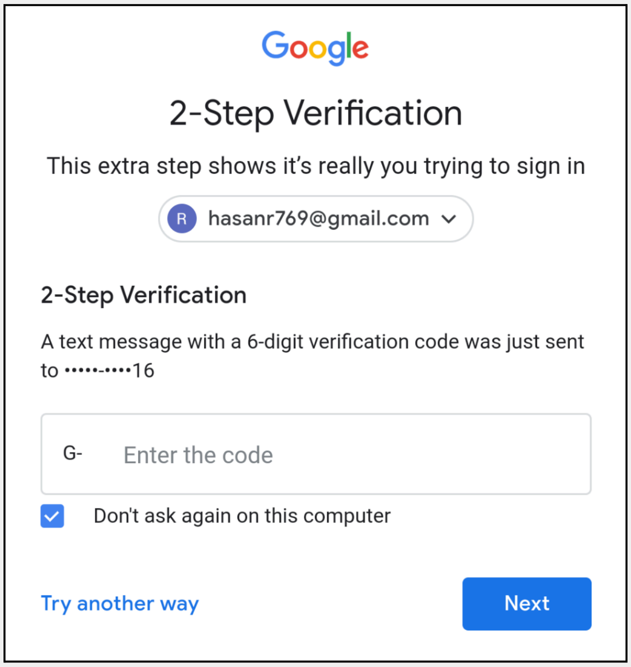
A 6-digit code may be sent to a number you've previously provided. Codes can be sent in a text message (SMS) or through a voice call, depending on the setting you chose. To verify it's you, enter the code on the sign-in screen.



2:48 PM

G-479842 is your Google verification code.

32 min



2-Step Verification

This extra step shows it's really you trying to sign in

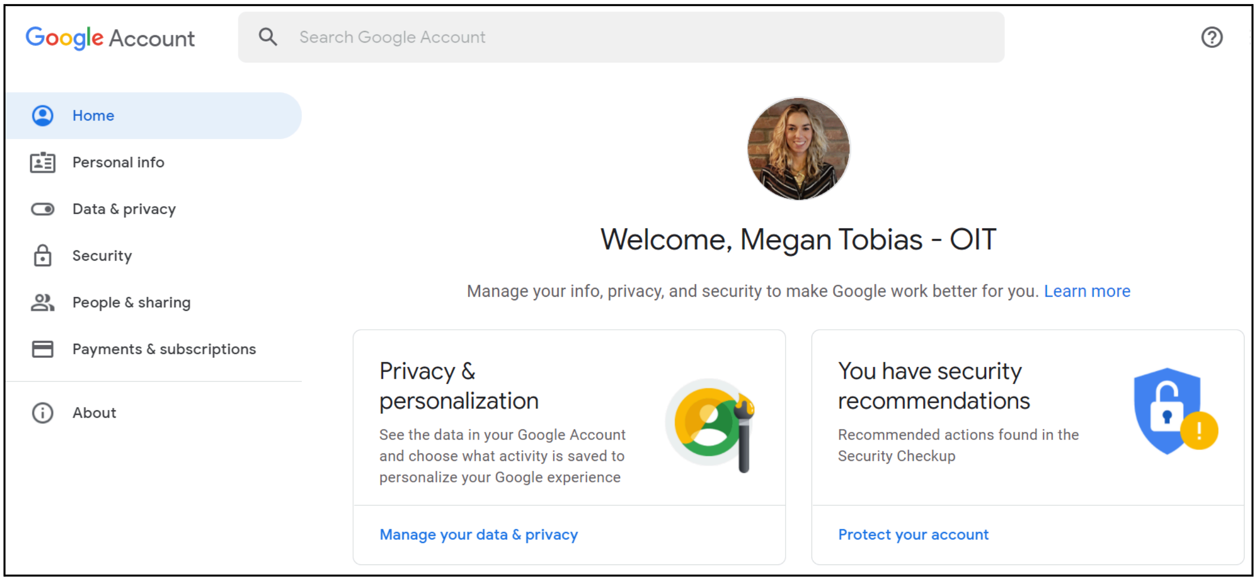
hasanr769@gmail.com

2-Step Verification

A text message with a 6-digit verification code was just sent to •••••-••••16

G- Enter the code

☑ Don't ask again on this computer



Welcome, Megan Tobias - OIT

Manage your info, privacy, and security to make Google work better for you. Learn more

Privacy & personalization

See the data in your Google Account and choose what activity is saved to personalize your Google experience

Manage your data & privacy

You have security recommendations

Recommended actions found in the Security Checkup

Protect your account

How long is the code good for when sent?

The code is only valid for a short time duration -- as it is meant to be used immediately to login.

Is my phone subject to CORA if I receive a text message from Google?

No, if you use your personal phone to receive your 2FA code, the information on your phone will not be subject to a CORA request.

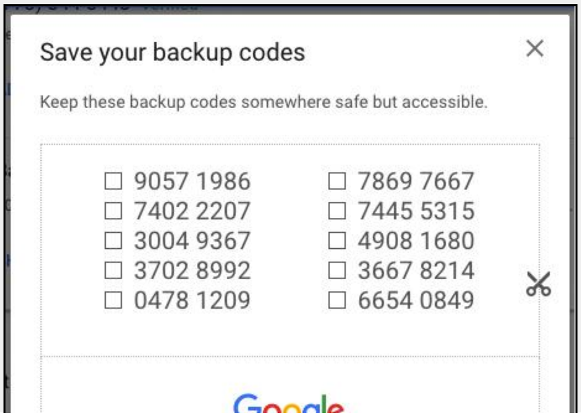
Option 2: Use Google Authenticator

You can set up Google Authenticator that creates one-time verification codes when you don't have an internet connection or mobile service.

Enter the verification code on the sign-in screen to help verify it's you.

Option 3: Use Backup Codes

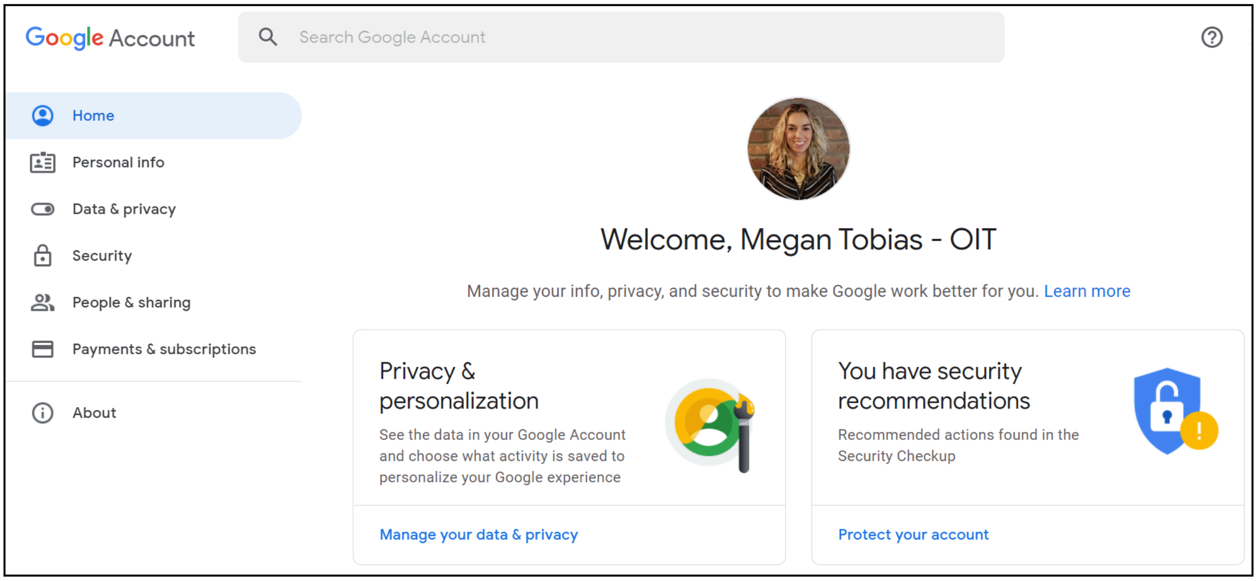
You can print or download a set of 8-digit backup codes to keep in a safe place. Backup codes are helpful if you lose your phone.



Save your backup codes

Keep these backup codes somewhere safe but accessible.

- ☐ 9057 1986
- ☐ 7402 2207
- ☐ 3004 9367
- ☐ 3702 8992
- ☐ 0478 1209
- ☐ 7869 7667
- ☐ 7445 5315
- ☐ 4908 1680
- ☐ 3667 8214
- ☐ 6654 0849



Welcome, Megan Tobias - OIT

Manage your info, privacy, and security to make Google work better for you. Learn more

Privacy & personalization

See the data in your Google Account and choose what activity is saved to personalize your Google experience

Manage your data & privacy

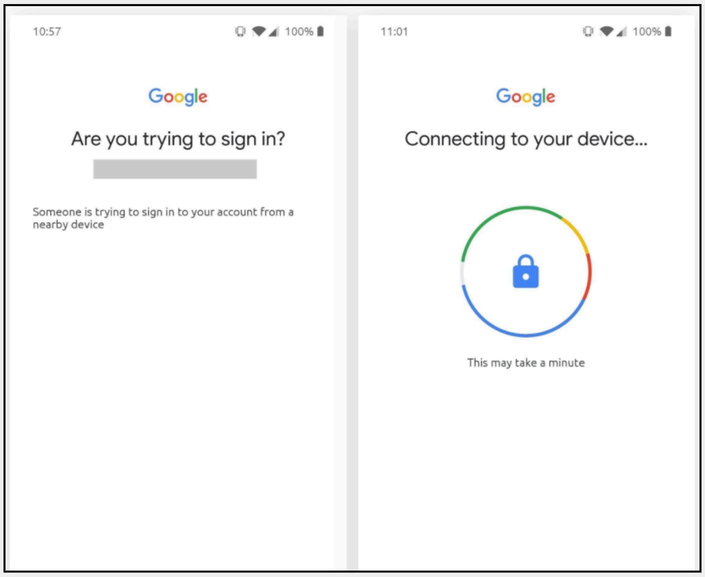
You have security recommendations

Recommended actions found in the Security Checkup

Protect your account

Option 4: Use the Built-in Security Key

A security key is a verification method that allows you to securely sign in. These are already built into your phone and Google will use Bluetooth to access it.



Are you trying to sign in?

Someone is trying to sign in to your account from a nearby device

Connecting to your device...

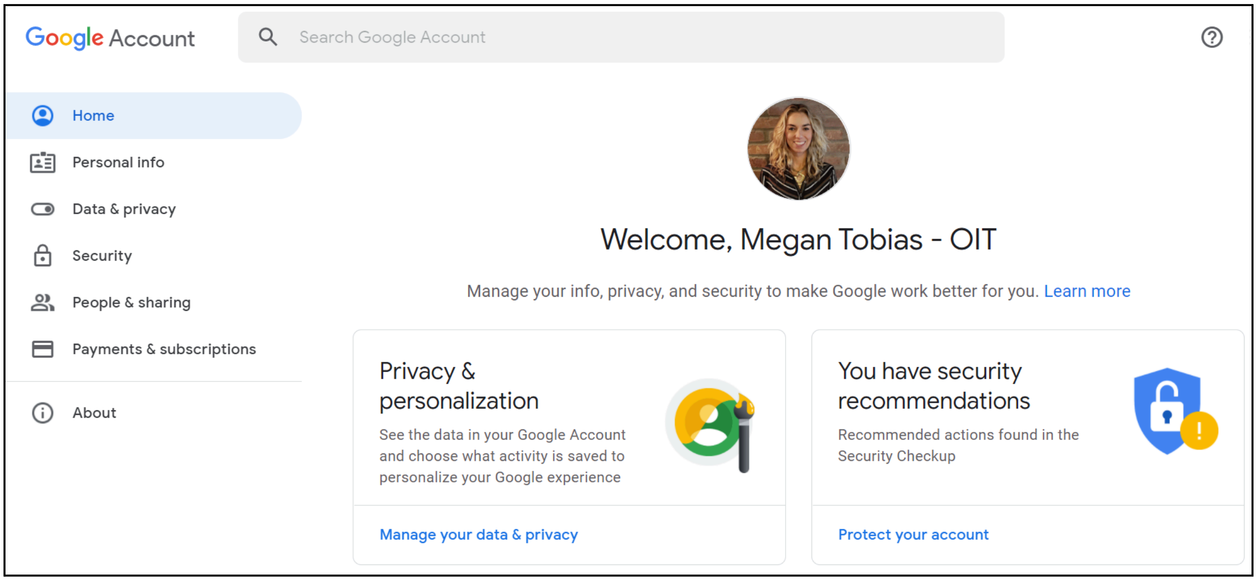
This may take a minute

Additional Questions

What happens if I don’t follow the prompts to enroll in 2FA?

You will be locked out of your work email account on Jan. 31, 2022 if you have not enrolled in 2FA. If you are locked out, you can use the Google Authenticator to generate a passcode and unlock your Gmail account. After that step you will need to go to myaccount.google.com/security and follow the standard procedure for enrolling with your mobile device.

What about my other devices like my smartphone or my home computer?



Welcome, Megan Tobias - OIT

Manage your info, privacy, and security to make Google work better for you. Learn more

Privacy & personalization

See the data in your Google Account and choose what activity is saved to personalize your Google experience

You have security recommendations

Recommended actions found in the Security Checkup

After the initial setup, you will be prompted to enter a code the first time you access your work email from a new device such as your home computer. You will also need to set up 2FA on your work or personal cell phone if you use it to access your work email.

Will all county workers be required to enroll in 2FA?

Yes; all county workers are required to enroll in 2FA by Jan. 31, 2022.

Will I need a code for a shared/group mailbox?

2FA will be applied to shared/group mailboxes.

If you access a shared mailbox by clicking on your profile icon and you see “(delegated)” next to the mailbox name then you will not need to enter a verification code. |

If you are the owner of a shared/group mailbox, then you will need to set up 2FA for that mailbox the same way you did for your individual work Google account.

In these cases we suggest that an official owner be designated for the shared/group inbox. If you do find that there are multiple people that need to sign in formally to the shared/group inbox, the owner can print a set of backup codes that can be shared among those that need to access the mailbox. The codes can be entered in any order and can be entered by any individual with access to the shared inbox but each code is only good for one use.

What if I don’t receive a code and end up locked out of my account?

Contact the OIT Service Desk: Call 303.239.HELP, Online at OIT Customer Service Portal or email.