

Two Factor Authentication

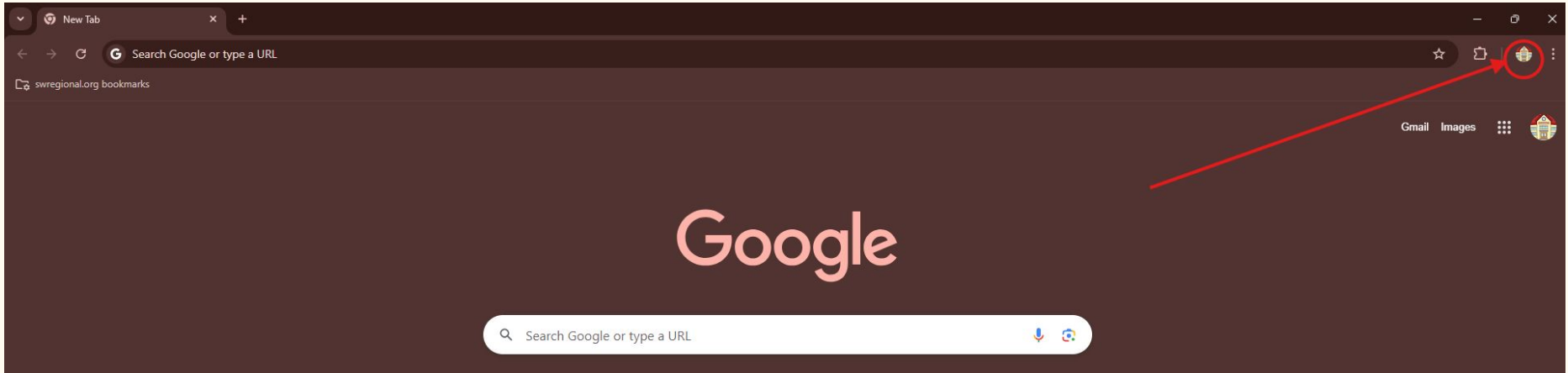
—

Two-factor Authentication/Multi-factor authentication - Continued

Below are the steps to enable 2FA/MFA on your google account:

1. Navigate to your Google Chrome Profile
2. Select “Manage your Google Account”
3. Select “Security & sign-in” on the left menu
4. Scroll down and select “2 step verification”
5. Select “Phone Number” under “Second steps” and add your cell phone number.
6. Fill out your phone number, select “Receive codes by text message” and then select “next”
7. Wait for a code to be sent your mobile device and enter the code in the box **if prompted**. *If the code includes a “G -” you don’t need that G, just the 6 digit code*
8. Once your number is added, navigate back and select the blue “Turn on 2-step Verification” button
9. You are all set!

For a visual representation on how to set up 2FA on your Google account, see slides 3 - 13





Google Account



Home



Personal info



Security & sign-in



Google password



Linked apps



Data & privacy



People & sharing



Wallet & subscriptions



Teacher Joe



Search Google Account



Transfer your content

Transfer your email and Google Drive files to another Google Account

Dismiss

Start transfer

How you sign in to Google

Make sure you can always access your Google Account by keeping this information up to date



2-Step Verification

2-Step Verification is off



Password

Last changed Sep 5, 2024



Skip password when possible

In this case, the user was prompted to sign on first. This is all dependent if you recently logged into your Google account.



Hi Teacher

 teacherjoe@swregional.org ▼

To continue, first verify it's you

Enter your password

☐ Show password

[Forgot password?](#) [Next](#)

English (United States) ▼

[Help](#) [Privacy](#) [Terms](#)

← 2-Step Verification

Turn on 2-Step Verification

Prevent hackers from accessing your account with an additional layer of security.

Unless you're signing in with a passkey, you'll be asked to complete the most secure second step available on your account. You can update your second steps and sign-in options any time in your settings. [Go to Security Settings](#) ➞



Second steps

Make sure you can access your Google Account by keeping this information up to date and adding more sign-in options



Passkeys and security keys



Add a passkey



Google prompt



Authenticator



Add authenticator app



Phone number



Add a phone number



Turn on 2-Step Verification

← 2-Step Verification phones

You can add phone numbers to get sign-in codes and security alerts.

+ Add phone number

Add a phone number

A phone number can be used to verify it's you when signing in and to receive alerts if there's unusual activity.



You can use a Google Voice number, but you won't be able to receive codes if you lose access to your Google Account. Charges from your carrier may apply. [Learn more about how Google uses this info](#)



Receive codes by text message



Receive codes by voice message

Cancel

Next

← 2-Step Verification phones

You can add phone numbers to get sign-in codes and security alerts.

[+ Add phone number](#)



Confirm your phone number

Make sure [REDACTED] is the number you would like to save. When you need to use your phone number to verify it's you signing in, codes will be sent to this number by text message.

[Back](#)

[Save](#)

← 2-Step Verification phones

You can receive sign-in codes at these numbers. You may have additional numbers that can be used to recover your Google Account. [Manage recovery phones](#)



(973)



+ Add a backup 2-Step Verification phone

← 2-Step Verification

Turn on 2-Step Verification

Prevent hackers from accessing your account with an additional layer of security.

Unless you're signing in with a passkey, you'll be asked to complete the most secure second step available on your account. You can update your second steps and sign-in options any time in your settings. [Go to Security Settings](#)



Second steps

Make sure you can access your Google Account by keeping this information up to date and adding more sign-in options



Passkeys and security keys



Add a passkey



Google prompt



Authenticator



Add authenticator app



Phone number



Turn on 2-Step Verification

You're now protected with 2-Step Verification



When signing in you'll be asked to complete the most secure second step, so make sure this info is always up to date



Phone number



Done

Password Security

It is important to always have a secure password on any account you are using. Short, non-complicated passwords can easily be breached. To prevent any attacks/hacks on your account it is important that your password meets the following criteria:

1. At least 8 characters—the more characters, the better
2. A mixture of both uppercase and lowercase letters
3. A mixture of letters and numbers
4. Inclusion of at least one special character, e.g., ! @ # ?]

*This criteria is a **strong** recommendation*

Passwords such as “1234”, “password” or anything less than 8 characters and common are **NOT** recommended as they can leave you vulnerable to being hacked.