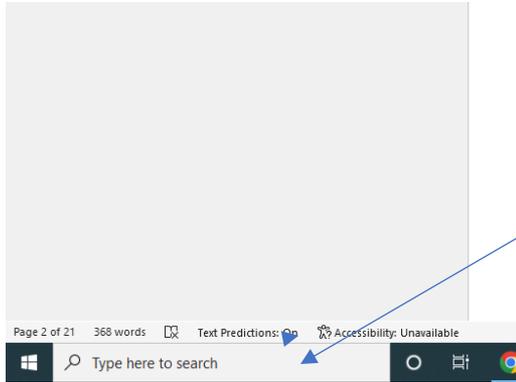


If you are planning to use the Google Authenticator app, go to the Apple app store or the Google app store and download the Google Authenticator app.



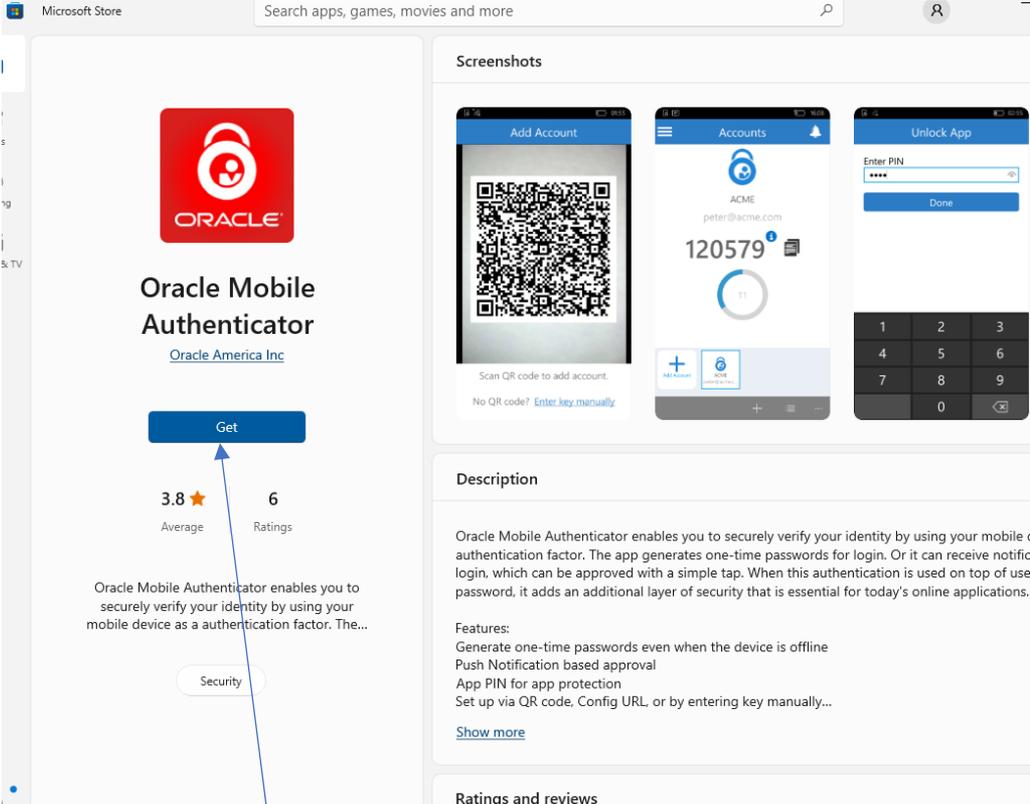
Google Authenticator

If you are using the Oracle authenticator on a Windows computer, click in the Search Window by the Start button



and type in “Store” with out the quotes and launch the Microsoft Store app. Once the Microsoft store opens, Search for “Oracle Mobile Authenticator”.

Microsoft Store Search apps, games, movies and more



The image shows the Microsoft Store page for the Oracle Mobile Authenticator app. At the top left is the Microsoft Store logo and a search bar. The app's logo, a red square with a white padlock and the word "ORACLE" below it, is prominently displayed. Below the logo is the app name "Oracle Mobile Authenticator" and the developer "Oracle America Inc". A blue "Get" button is centered below the app name. To the right of the button, the app has a 3.8 star average rating from 6 reviews. A blue arrow points from the text "Click 'Get'" at the bottom left of the image to the "Get" button. Below the button is a "Security" badge. To the right of the main app information is a "Screenshots" section with three mobile app interface images: "Add Account" (QR code), "Accounts" (showing an account for ACME with email peter@acme.com and a 120579 one-time password), and "Unlock App" (PIN entry screen). Below the screenshots is a "Description" section with a paragraph about the app's security features, a "Features" list, and a "Show more" link. At the bottom of the page is a "Ratings and reviews" section.

## Oracle Mobile Authenticator

Oracle America Inc

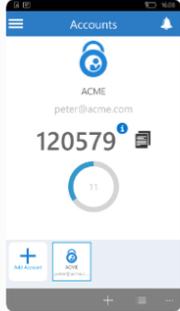
Get

3.8 Average Rating 6 Ratings

Oracle Mobile Authenticator enables you to securely verify your identity by using your mobile device as a authentication factor. The...

Security

### Screenshots



### Description

Oracle Mobile Authenticator enables you to securely verify your identity by using your mobile authentication factor. The app generates one-time passwords for login. Or it can receive notification based approval. When this authentication is used on top of your password, it adds an additional layer of security that is essential for today's online applications.

#### Features:

- Generate one-time passwords even when the device is offline
- Push Notification based approval
- App PIN for app protection
- Set up via QR code, Config URL or by entering key manually...

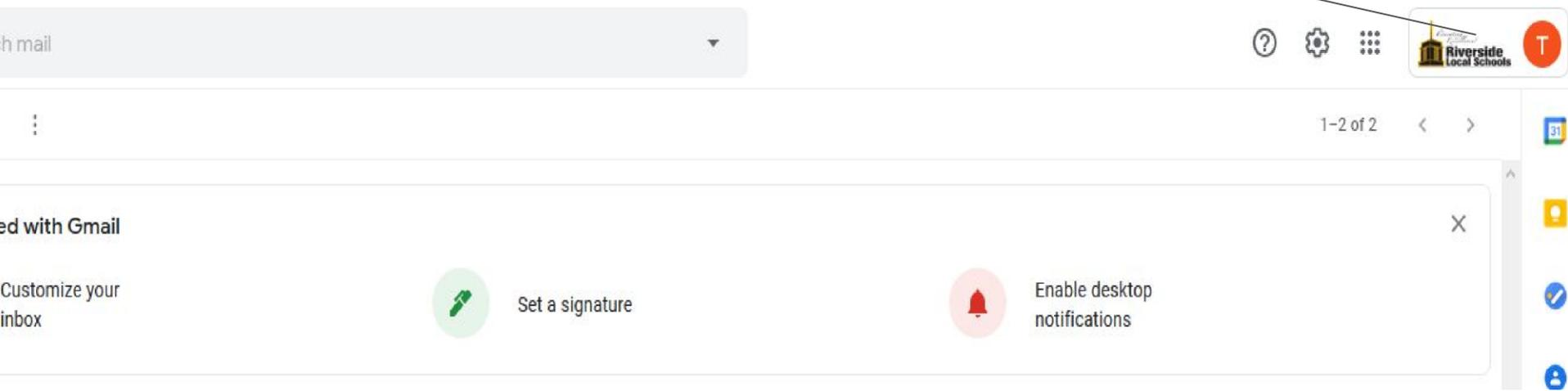
[Show more](#)

### Ratings and reviews

Click "Get"

Configure your email for Multifactor Authentication. If you are using a Security Key, Stop and contact the Tech office.

Log into your Gmail account and click on your name at the top right



# Click on Manage your Google Account

This account is managed by riversideschools.net. [Learn more](#)



**Test Account**  
testaccount@riversideschools.net

[Manage your Google Account](#)

 Add another account

[Sign out](#)

able desktop  
ifications

are only avai

ir inbox, you

# Click on Security

-  Home
-  Personal info
-  Data & personalization
-  Security
-  People & sharing
-  Payments & subscriptions

---

-  About

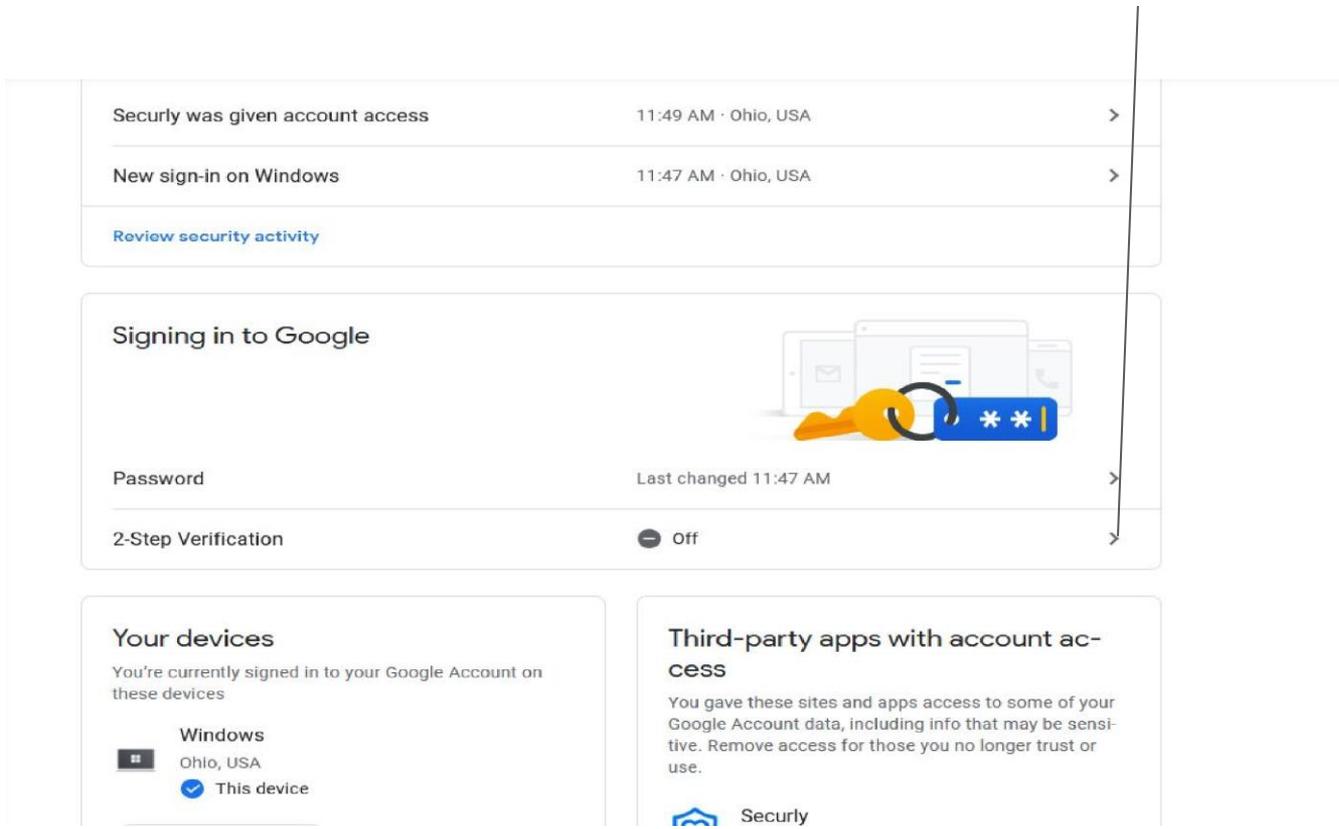
We

Manage your info, privacy, a

## Privacy & personalization

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

# Click on 2-Step Verification Arrow



The screenshot shows the Google Account Security settings page. At the top, there are two activity items: "Securely was given account access" and "New sign-in on Windows", both with right-pointing chevron arrows. Below these is a link for "Review security activity". The main section is titled "Signing in to Google" and features an illustration of a yellow key and a blue security key. Underneath, there are two settings: "Password" (last changed 11:47 AM) and "2-Step Verification" (currently "Off"). A red arrow points to the right-pointing chevron arrow next to the "2-Step Verification" setting. Below the main section are two additional panels: "Your devices" (showing a Windows device) and "Third-party apps with account access" (with a "Security" link).

Securely was given account access	11:49 AM · Ohio, USA	>
New sign-in on Windows	11:47 AM · Ohio, USA	>
<a href="#">Review security activity</a>		

### Signing in to Google

Password Last changed 11:47 AM >

2-Step Verification Off >

#### Your devices

You're currently signed in to your Google Account on these devices

- Windows  
Ohio, USA  
 This device

#### Third-party apps with account access

You gave these sites and apps access to some of your Google Account data, including info that may be sensitive. Remove access for those you no longer trust or use.

[Security](#)

# Click the GET STARTED Button

← 2-Step Verification



**Protect your account with 2-Step Verification**

Each time you sign in to your Google Account, you'll need your password and a verification code. [Learn more](#)

 **Add an extra layer of security**

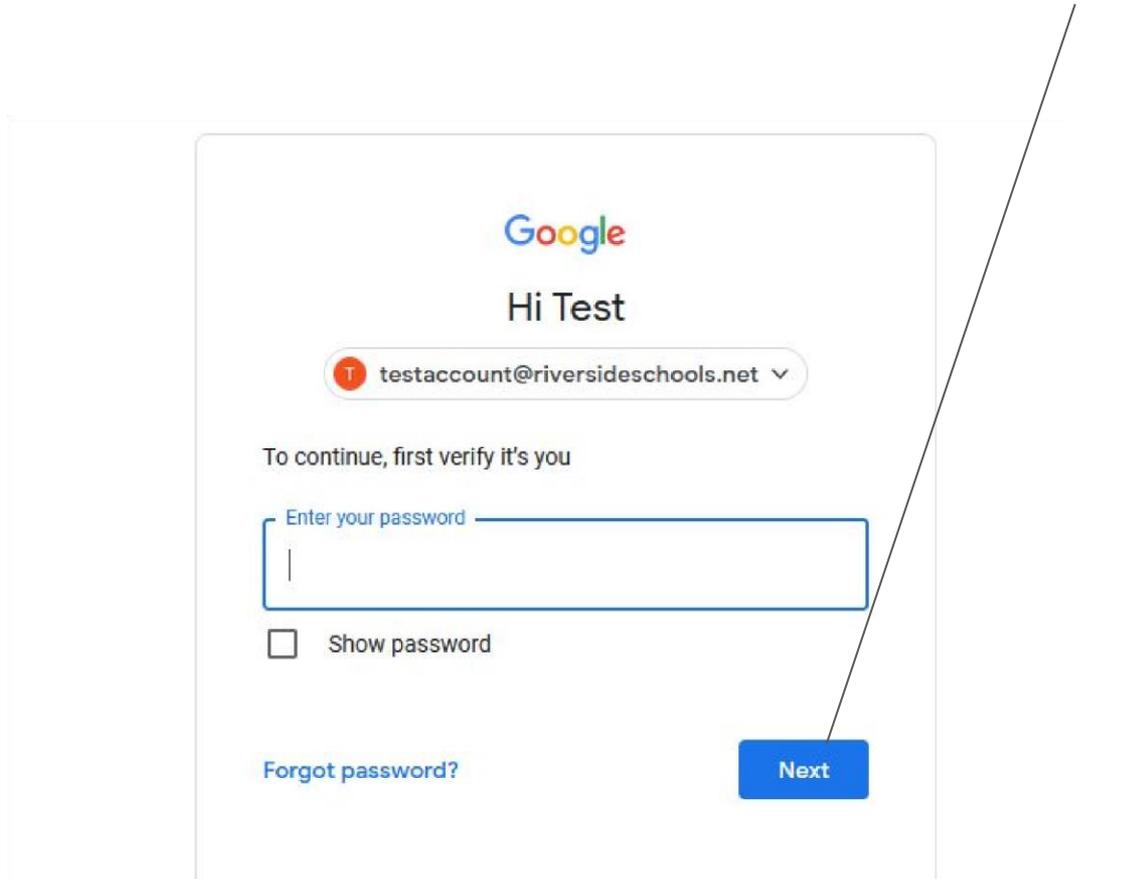
Enter your password and a unique verification code that's sent to your phone.

 **Keep the bad guys out**

Even if someone else gets your password, it won't be enough to sign in to your account.

[GET STARTED](#)

# Type in your password and click Next



The image shows a Google account login interface. At the top is the Google logo, followed by the text "Hi Test". Below this is a rounded rectangular field containing an email address "testaccount@riversideschools.net" with a dropdown arrow on the right. Underneath the email field is the instruction "To continue, first verify it's you". This is followed by a password input field with the placeholder text "Enter your password" and a vertical cursor. Below the password field is a checkbox labeled "Show password". At the bottom left is a link "Forgot password?". At the bottom right is a blue button labeled "Next". A thin black line originates from the top right of the "Next" button and extends diagonally upwards and to the right, crossing the top of the slide's text.

Google

Hi Test

testaccount@riversideschools.net

To continue, first verify it's you

Enter your password

Show password

[Forgot password?](#)

Next

Type in your phone number and choose how you would like to be notified, then click Next. If you are not using a cell phone, you will need to enter a phone number to receive the code from a phone call.

← 2-Step Verification



Let's set up your phone

What phone number do you want to use?

 111-111-1111

Google will only use this number for account security.  
Don't use a Google Voice number.  
Message and data rates may apply.

How do you want to get codes?

Text message  Phone call

[Show more options](#)

Step 1 of 3 [NEXT](#)

Type in the Code number that Google just sent to you,  
Then click Next

← 2-Step Verification



**Confirm that it works**

Google just sent a text message with a verification code to (449) [REDACTED].

Enter the code

123456

Didn't get it? [Resend](#)

[BACK](#) Step 2 of 3 [NEXT](#)

# Click TURN ON

← 2-Step Verification



**It worked! Turn on 2-Step Verification?**

Now that you've seen how it works, do you want to turn on 2-Step Verification for your Google Account `testaccount@riversideschools.net`?

Step 3 of 3

**TURN ON**

If you are using a phone number for Authentication, you have completed the setup for email. If you are using an Authenticator app, scroll down to Authenticator app and click Set up” If you are using backup codes, Click Setup and print your codes. If you would like to get a Google Prompt, click Add phone.

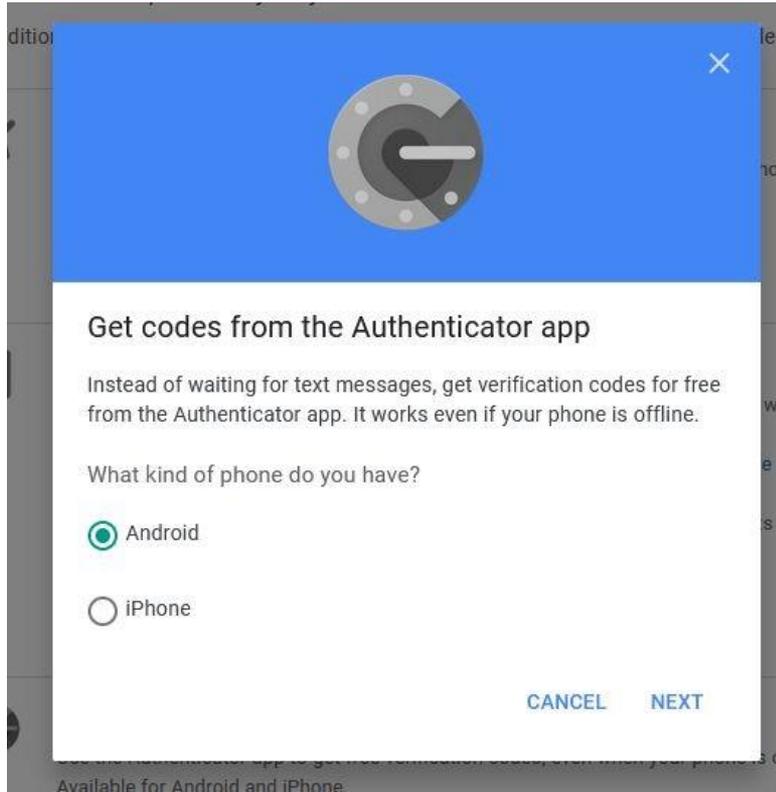
Add more second steps to verify it's you  
Set up additional backup steps so you can sign in even if your other options aren't available.

 **Backup codes**  
These printable one-time passcodes allow you to sign in when away from your phone, like when you're traveling.  
[SET UP](#)

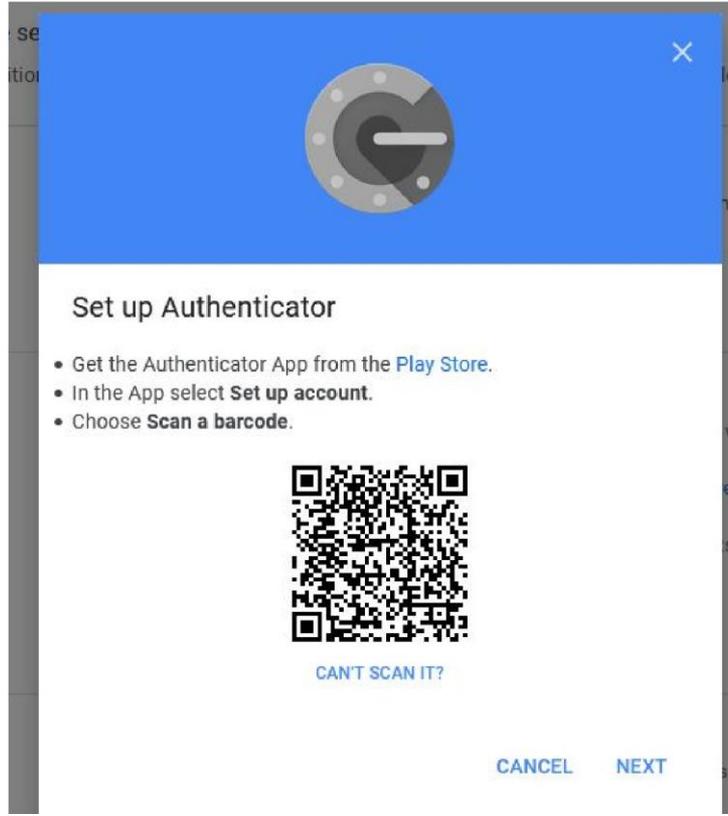
 **Google prompts**  
After you enter your password, Google prompts are securely sent to every phone where you're signed in. Just tap the notification to review and sign in.  
To stop getting prompts on a particular phone, sign out of that phone. [Learn more](#)  
**Note:** If you sign in to your Google Account on any eligible phone, Google prompts will be added as another method for 2-Step Verification.  
[ADD PHONE](#)

 **Authenticator app**  
Use the Authenticator app to get free verification codes, even when your phone is offline. Available for Android and iPhone.  
[SET UP](#)

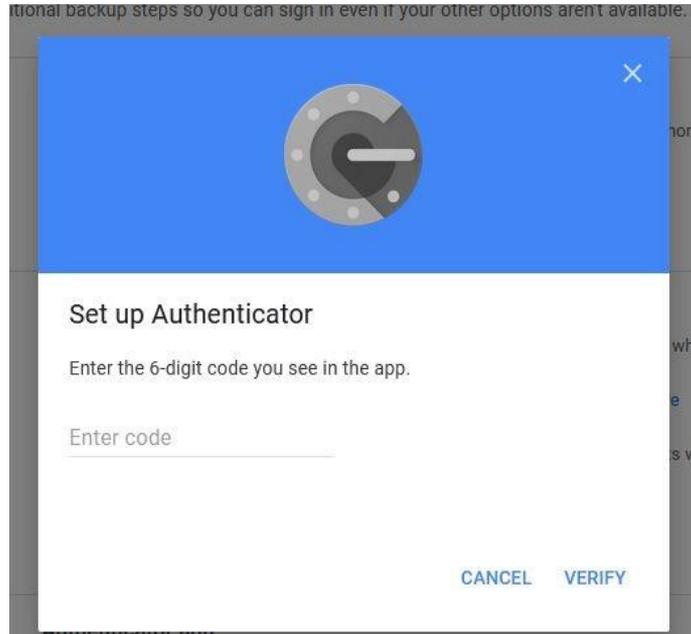
Google Authenticator: Choose your platform and click Next.



Open the Authenticator app, tap + to scan the QR Code and click Next

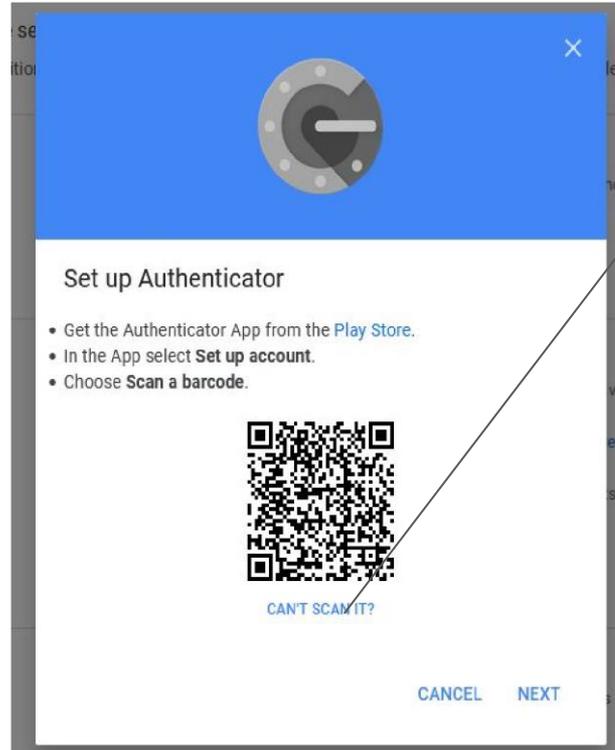


# Type in the 6 digit code and click Verify

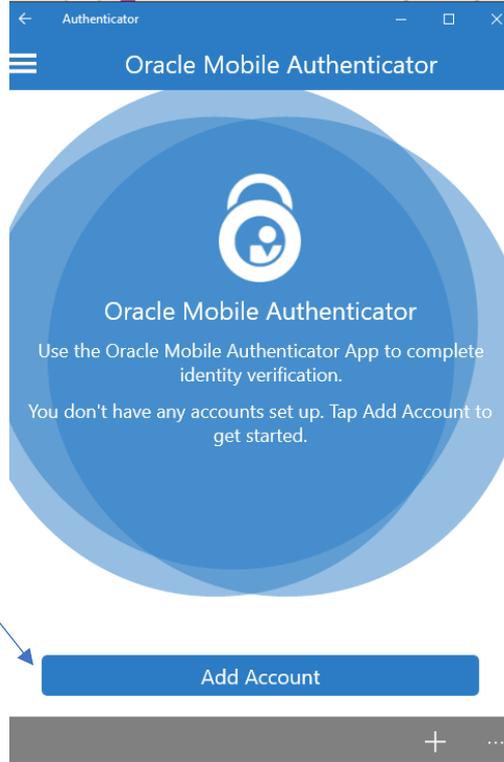


**Setup is complete and you can close the tab.**

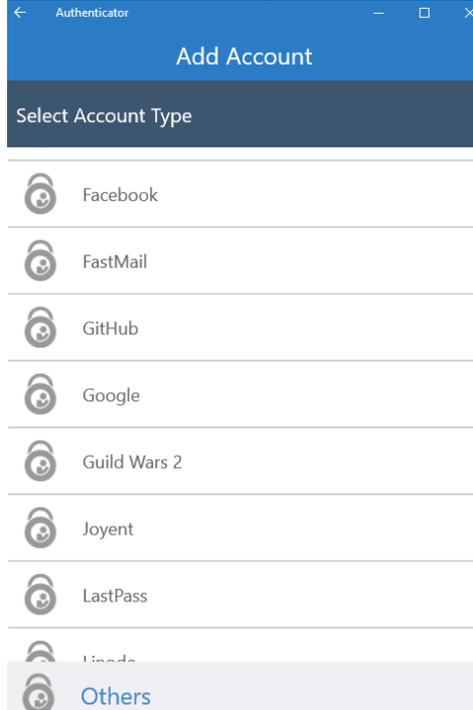
If you are using a PC for 2 step verification, Open the Oracle App and click “Cant Scan it?” under the QR Code



Open the Authentication app on your PC and click “Add account”.



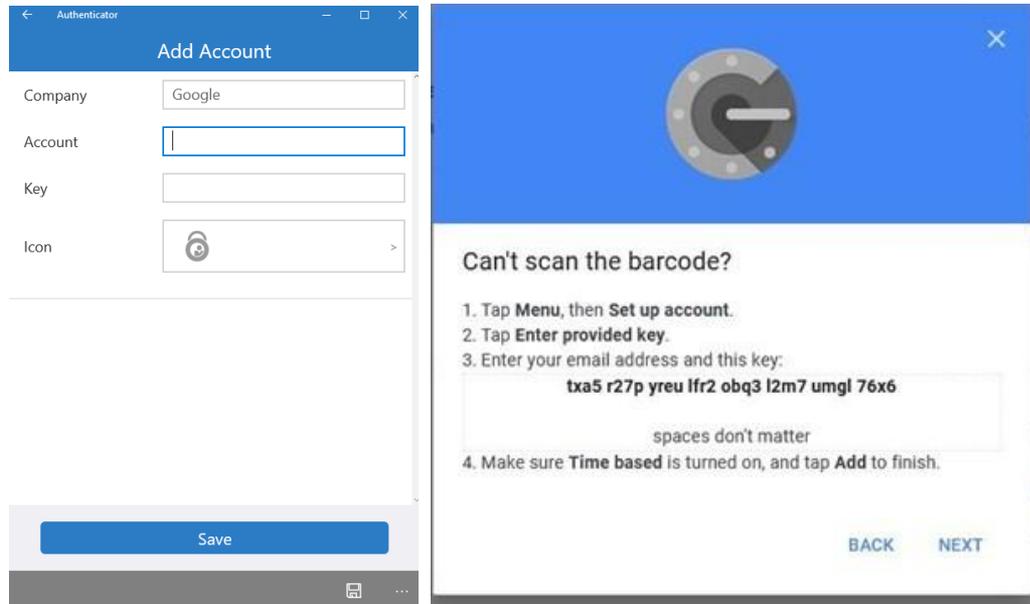
Click the “Enter Key Manually” Link. Choose Google from the list.



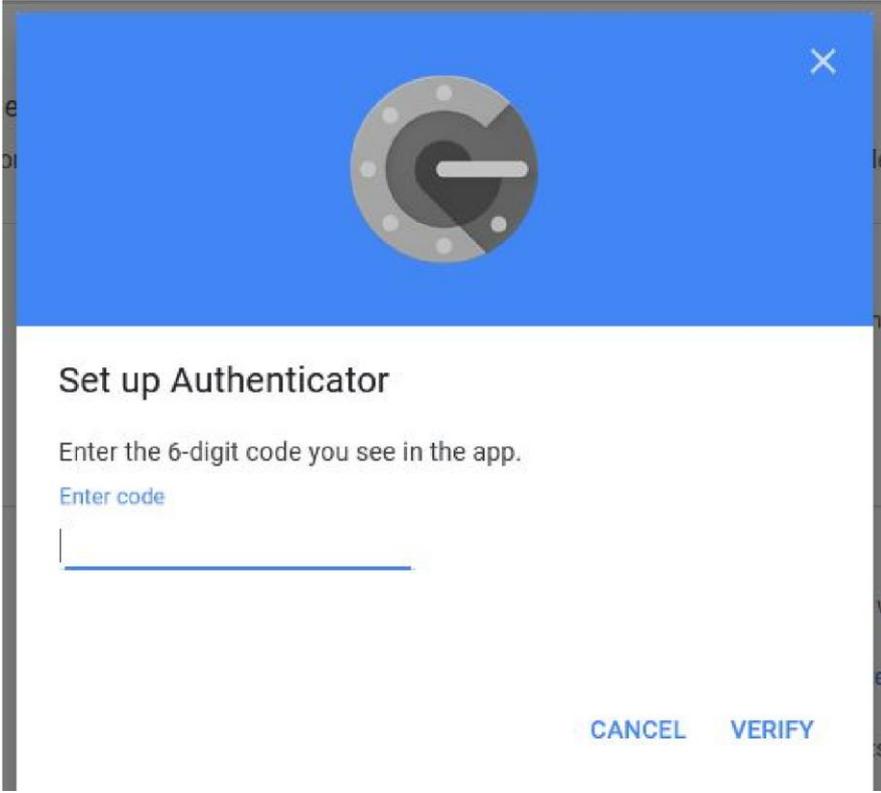
Scan QR code to add account.

No QR code? [Enter key manually](#)

Name the Account Gmail or work, etc... Copy the Key from the Gmail page and paste it into the Oracle Authenticator app. You do not need to enter your email address like it says on the Gmail page. Click the Arrow on the Icon Window and choose Google. Click Save on the Authenticator app and click Next on the Google Page.



Enter the code from the Oracle Authenticator on the Gmail screen and click Verify



Set up Authenticator

Enter the 6-digit code you see in the app.

[Enter code](#)

CANCEL VERIFY

Setup is complete. You can close the Tab.