



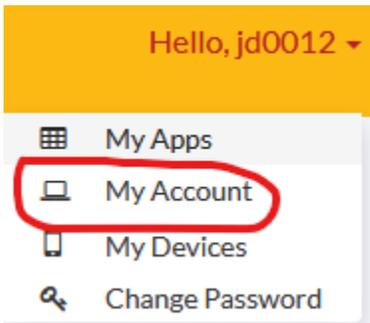
**Google Authenticator** is a software-based authenticator by Google that implements two-step verification services using the Time-based One-time Password Algorithm (TOTP; specified in RFC 6238) and HMAC-based One-time Password algorithm (HOTP; specified in RFC 4226), for authenticating users of software applications.

When logging into a site supporting Authenticator (including Google services) or using Authenticator-supporting third-party applications such as password managers or file hosting services, Authenticator generates a six- to eight-digit one-time password which users must enter in addition to their usual login details.

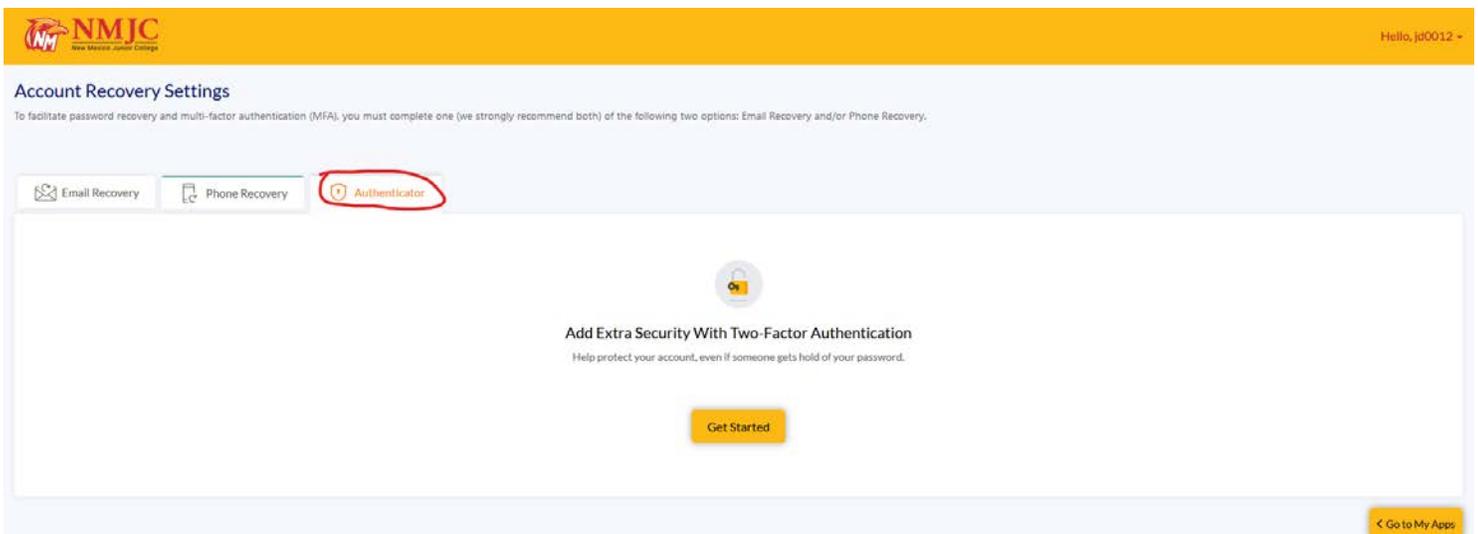
### ***How to set up Google Authenticator in the T-BirdWeb Portal?***

On your mobile device, download the Google Authenticator app from the Apple App Store (iOS) or Google Play Store (Android).

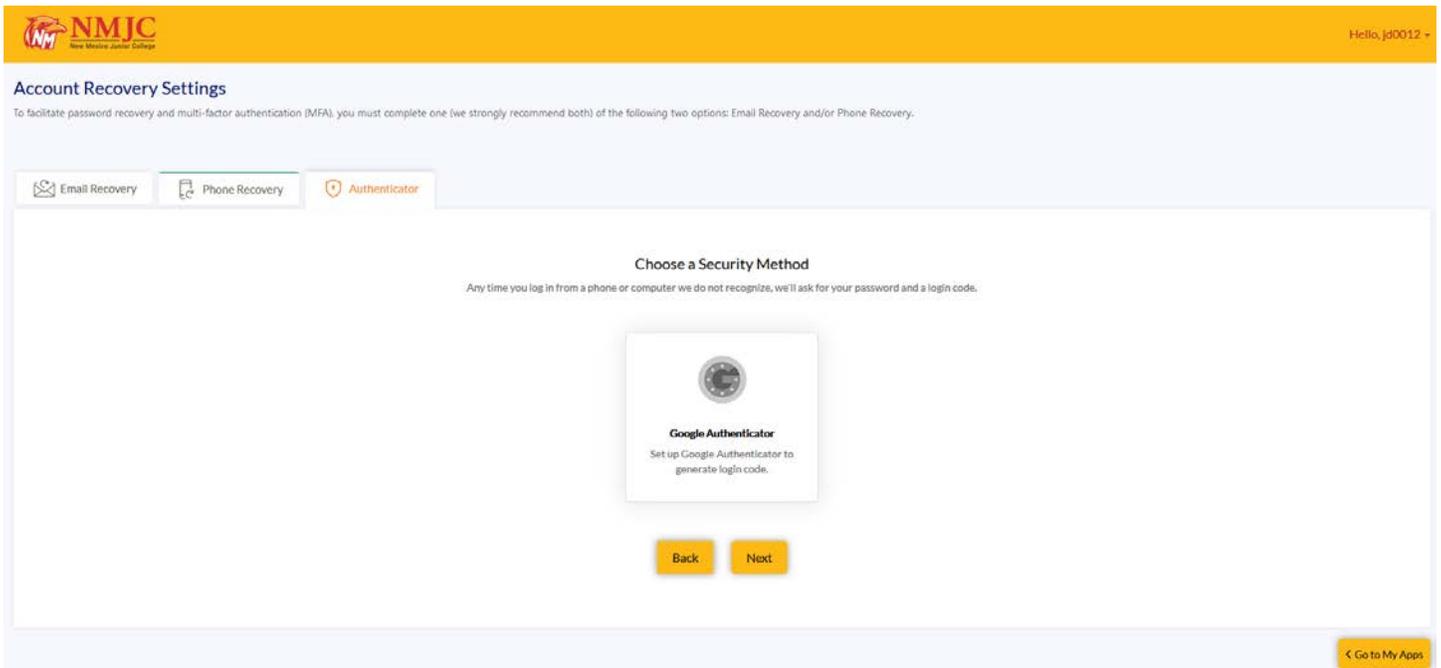
Using a device other than the device where the Google Authenticator app is installed, log in to the [T-BirdWeb Portal](#), click the drop-down menu located to the right of your Username, then click My Account and enter your password if prompted.



Click on the Authenticator tab. Click on Get Started.

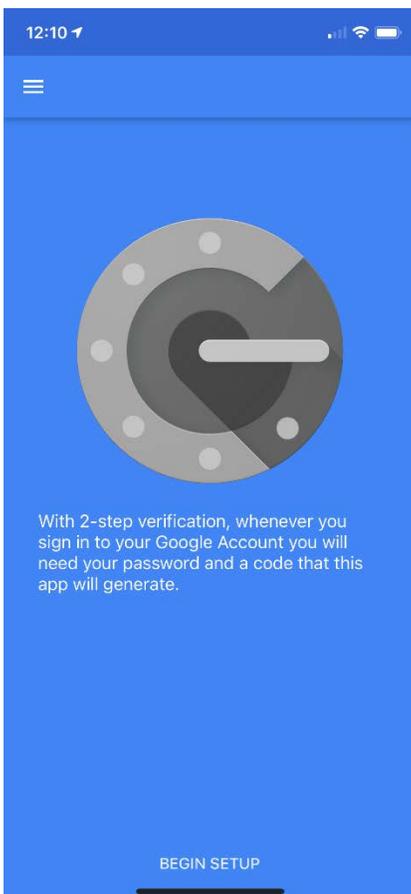


Click Next.

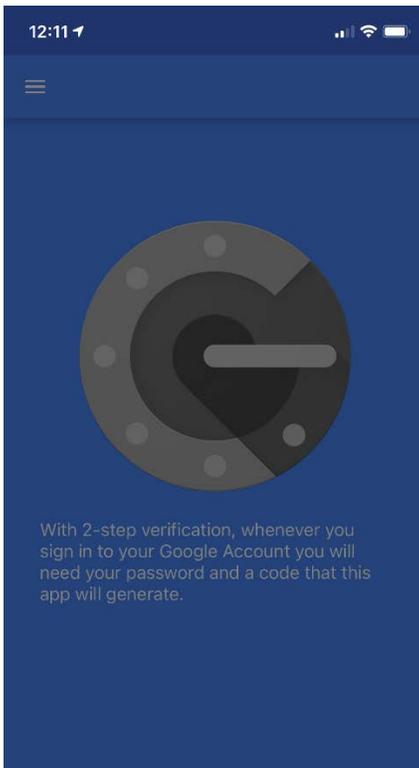


The screenshot shows a web interface for "Account Recovery Settings" on the NMJC (New Mexico Junior College) website. The page header includes the NMJC logo and the user name "Hello, jd0012". Below the header, there is a section titled "Account Recovery Settings" with a sub-header: "To facilitate password recovery and multi-factor authentication (MFA), you must complete one (we strongly recommend both) of the following two options: Email Recovery and/or Phone Recovery." There are three tabs: "Email Recovery", "Phone Recovery", and "Authenticator". The "Authenticator" tab is selected. The main content area is titled "Choose a Security Method" and contains the text: "Any time you log in from a phone or computer we do not recognize, we'll ask for your password and a login code." Below this text is a card for "Google Authenticator" with the sub-text: "Set up Google Authenticator to generate login code." At the bottom of the card are two buttons: "Back" and "Next". In the bottom right corner of the page, there is a button labeled "< Go to My Apps".

Open the Google Authenticator app on your mobile device and tap Begin Setup.



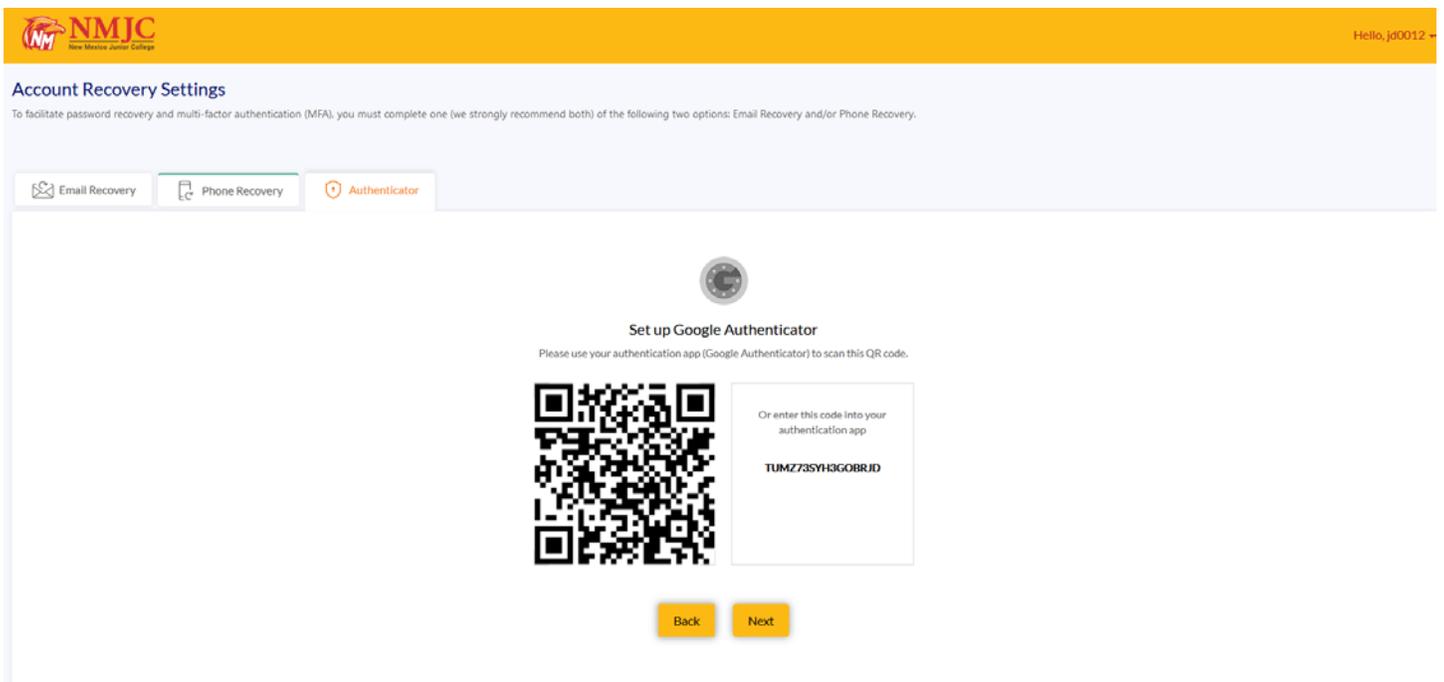
Tap Scan barcode.



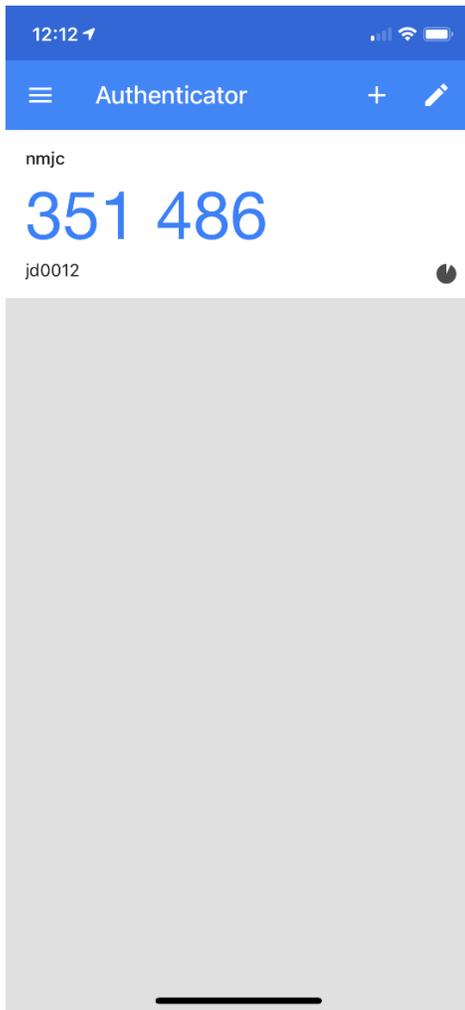
Scan barcode

Manual entry

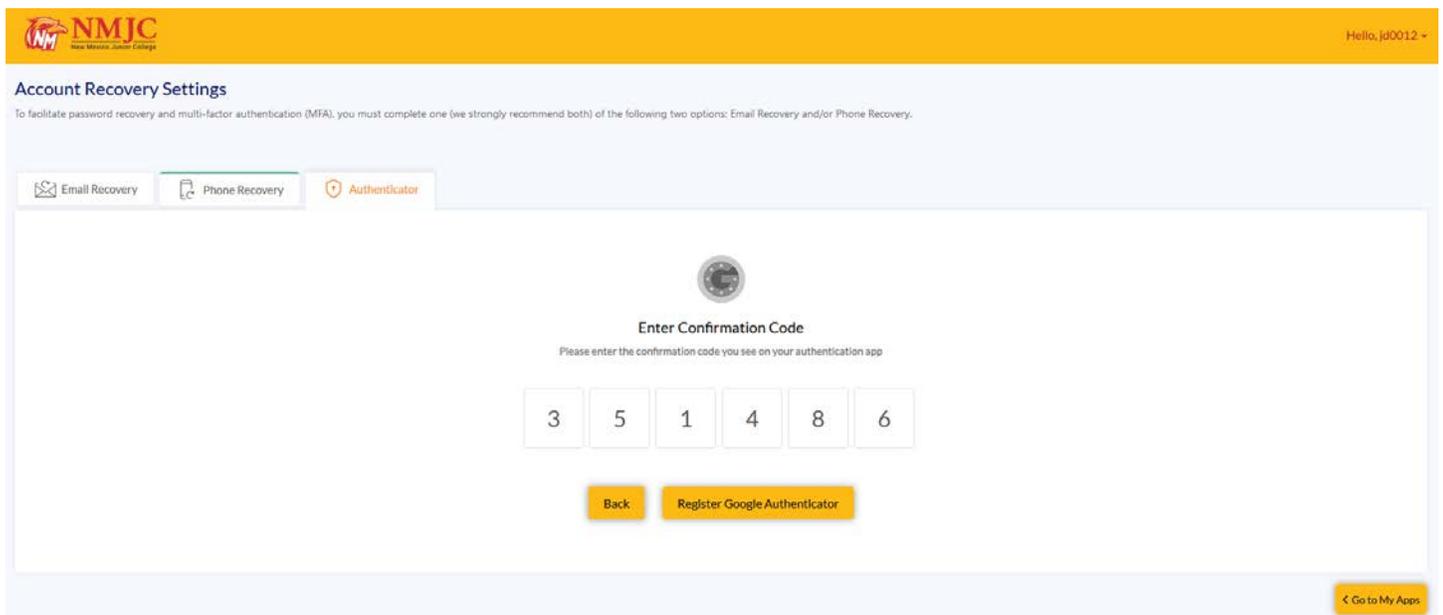
Point your mobile device's camera at the QR code on the screen.



If successful, your app will look like this.



Enter this code on your screen and then click Register Google Authenticator.



Confirm that the registration was successful.

Account Recovery Settings

To facilitate password recovery and multi-factor authentication (MFA), you must complete one (we strongly recommend both) of the following two options: Email Recovery and/or Phone Recovery.

Email Recovery Phone Recovery Authenticator

Google Authenticator registered successfully

**Google Authenticator**

Any time you log in from a phone or computer we do not recognize, we'll ask for your password and a login code.

Google Authenticator  
Set up Google Authenticator to generate login code.

De-register Google Authenticator

< Go to My Apps

Now, when you log in to the T-BirdWeb Portal or request a password reset, you will have this choice.



### Additional security verification

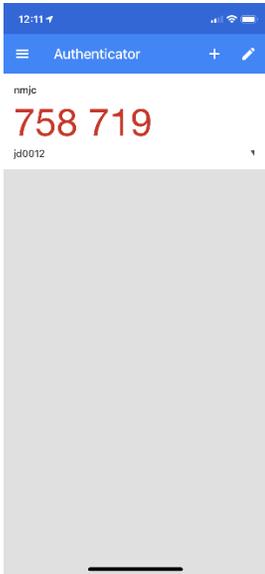
This is an extra layer of security to ensure that only you can access your account

Select a verification option

- T Send me a Text Message >
- G Use Google Authenticator >**

Open the Google Authenticator app on your phone and enter the code. If you are using a device that you trust, make sure you check the ***Trust this device*** checkbox before you click the Submit button.

Note: The code will change often.



< Back



### Google Authenticator security verification

This is an extra layer of security to ensure that only you can access your account

Please verify using Google Authenticator installed on your registered device by entering the security code

Enter verification code

Submit

Trust this device