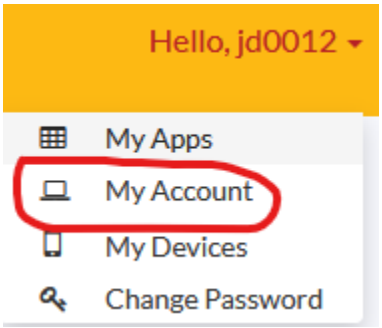
Google Authenticator is a software-based authenticator by Google that implements two-step verification services using the Time-based One-time Password Algorithm (TOTP; specified in RFC 6238) and HMAC-based One-time Password algorithm (HOTP; specified in RFC 4226), for authenticating users of software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

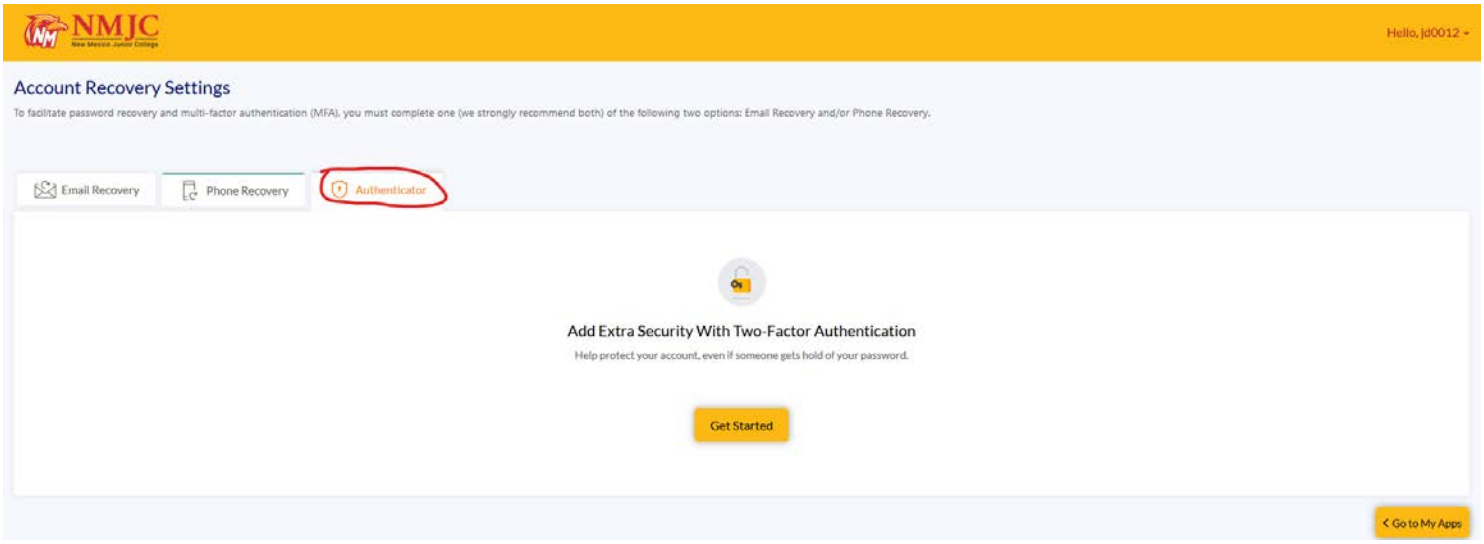
How to set up Google Authenticator in the T-BirdWeb Portal?

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

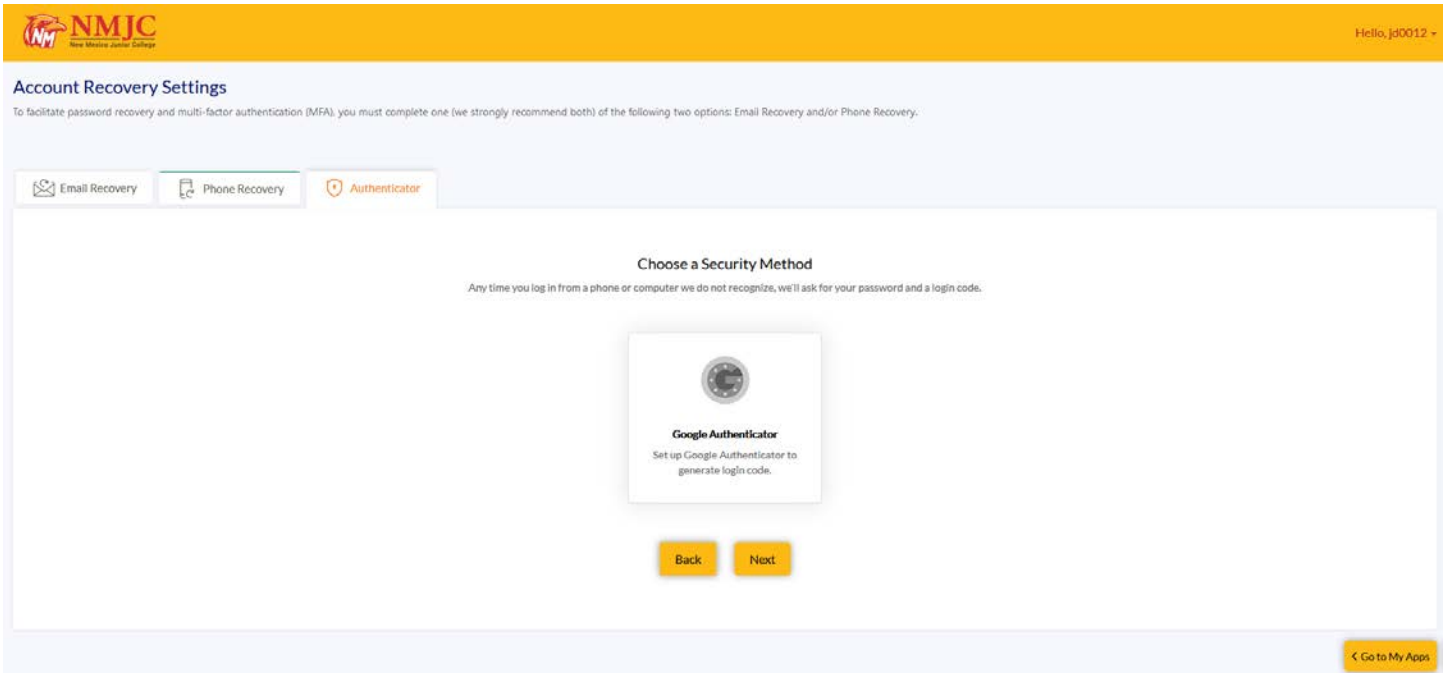
Using a device other than the device where the Google Authenticator app is installed, log in to the T-BirdWeb Portal, click the drop-down menu located to the right of your Username, then click My Account and enter your password if prompted.



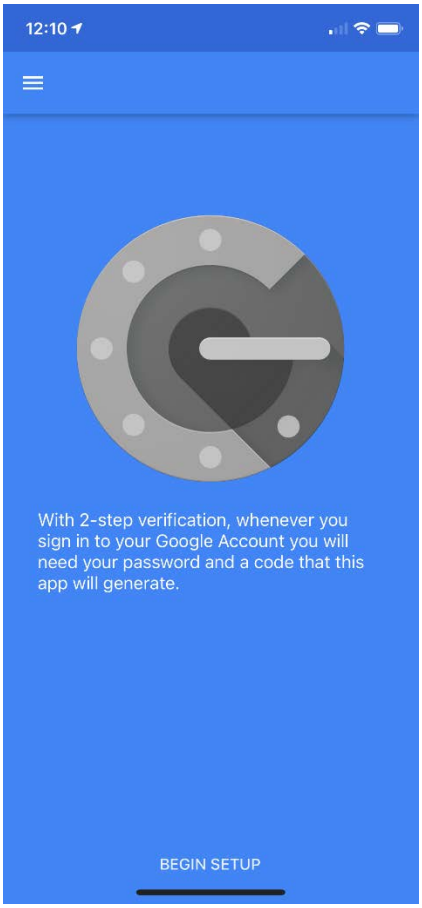
Click on the Authenticator tab. Click on Get Started.



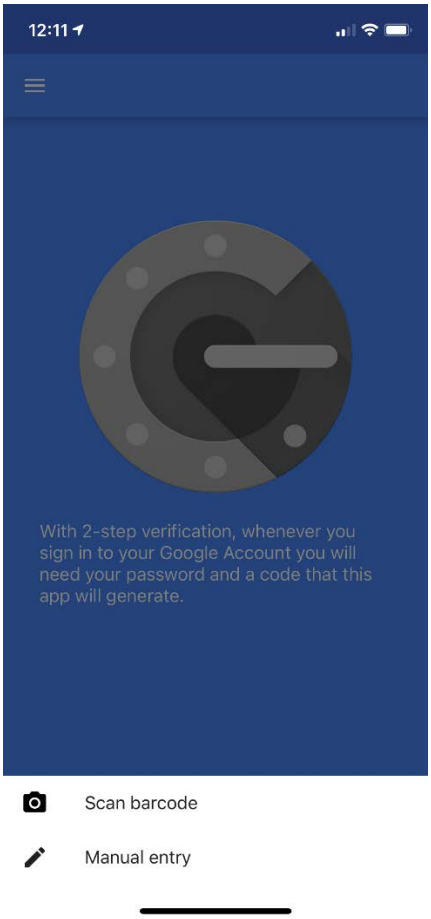
Click Next.



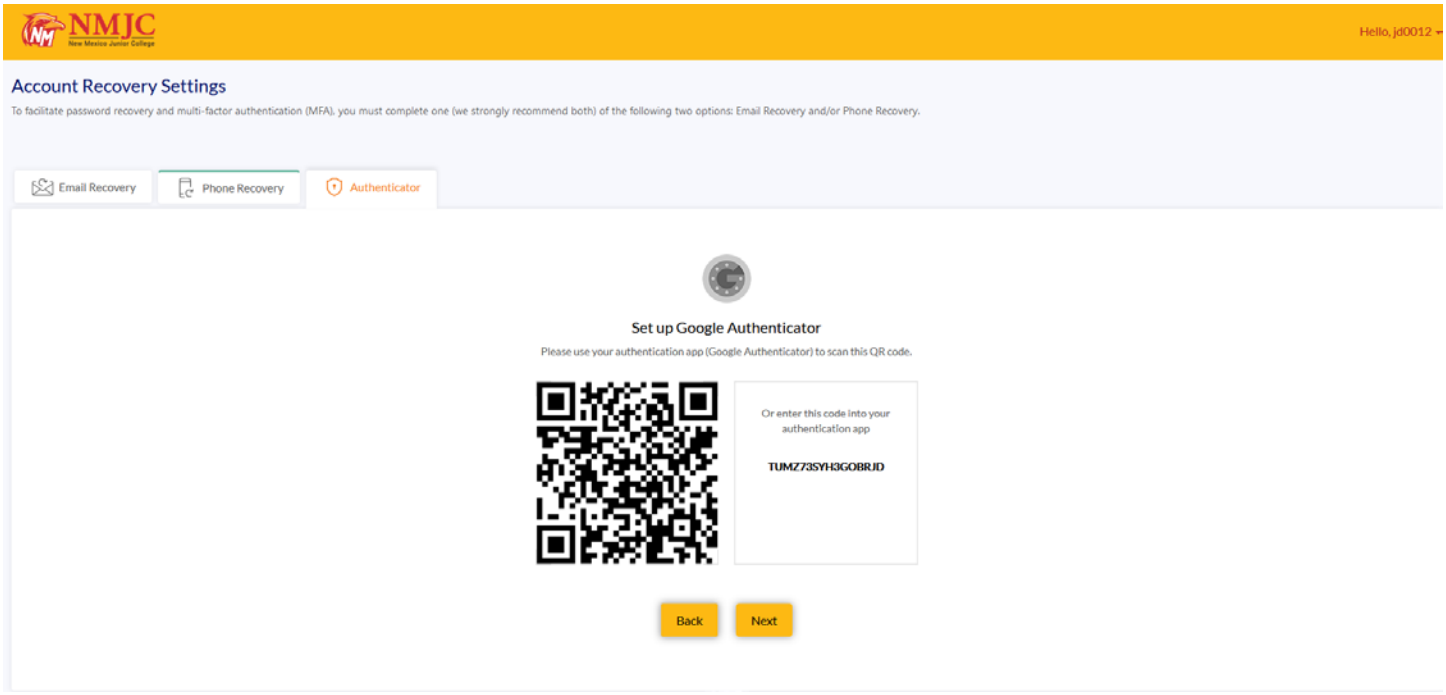
Open the Google Authenticator app on your mobile device and tap Begin Setup.



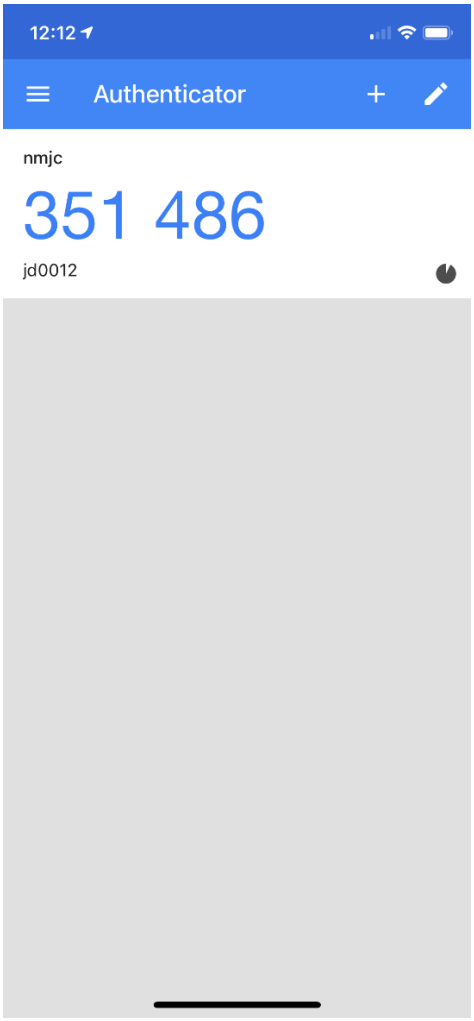
Tap Scar barcode.



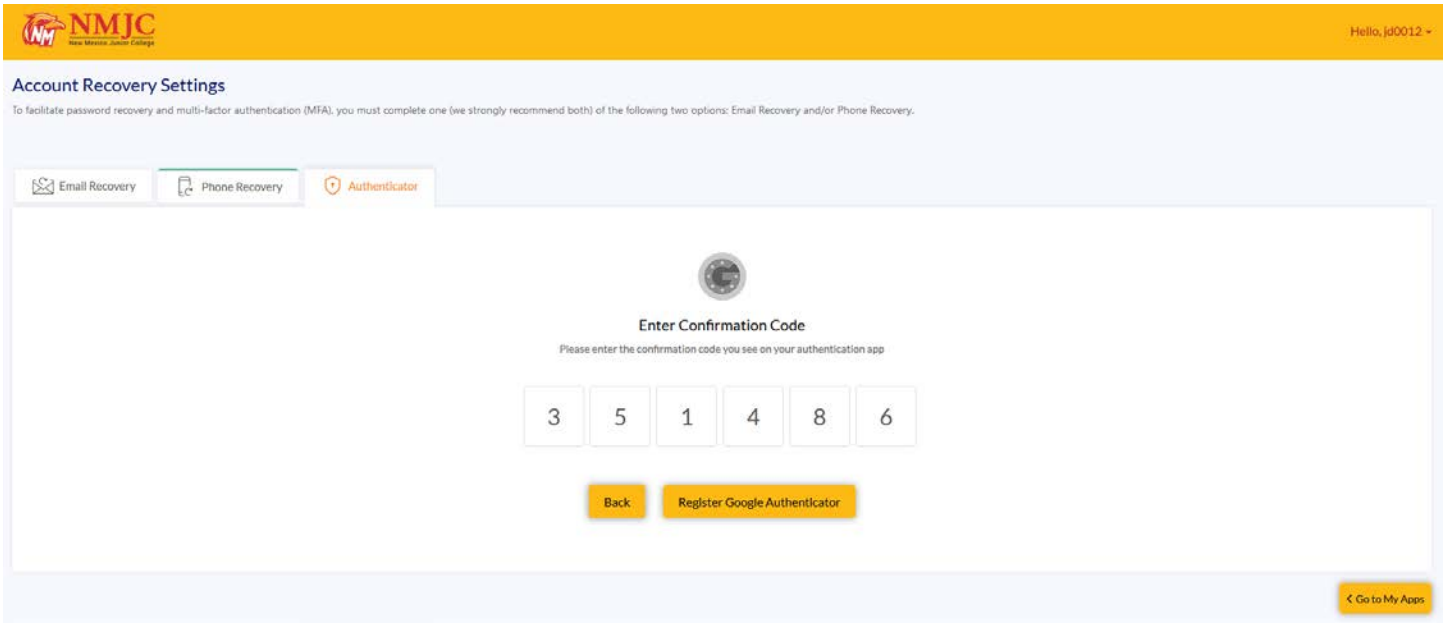
Point your mobile device’s camera at the QR code on the screen.



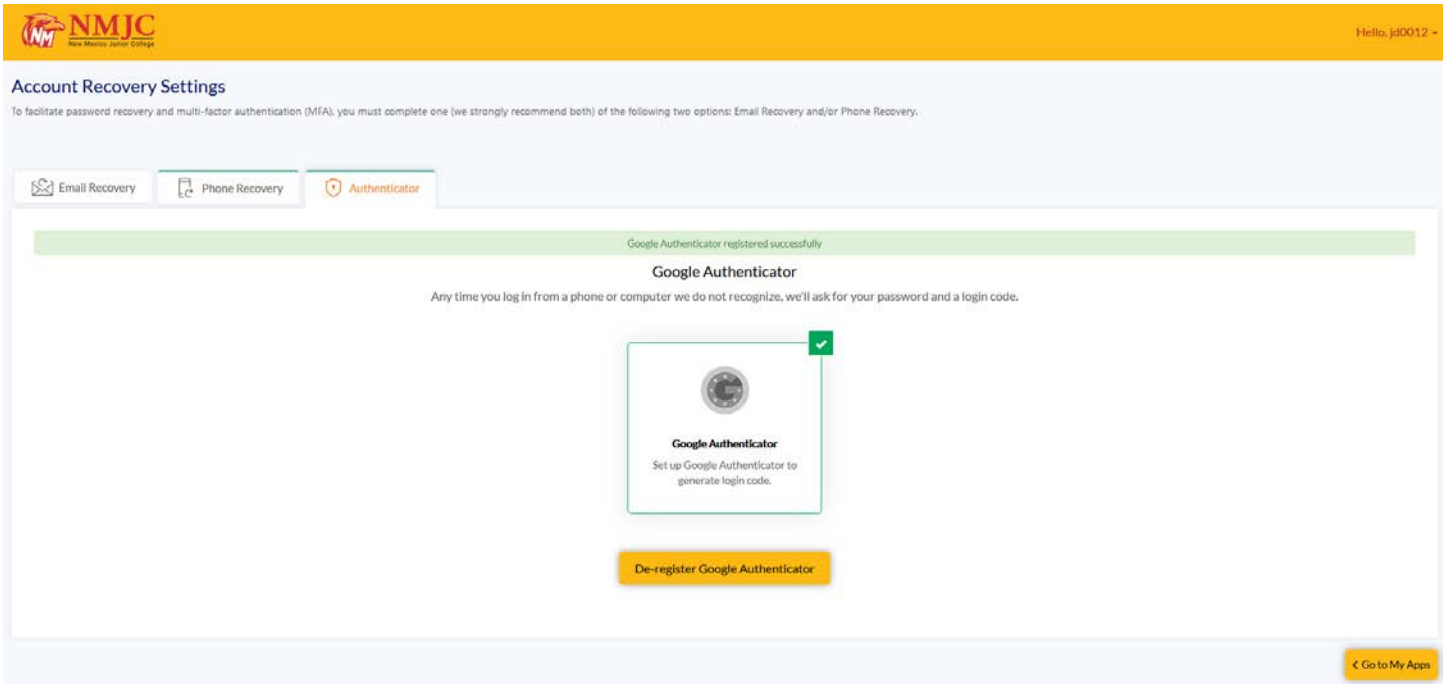
If successful, your app will look like this.



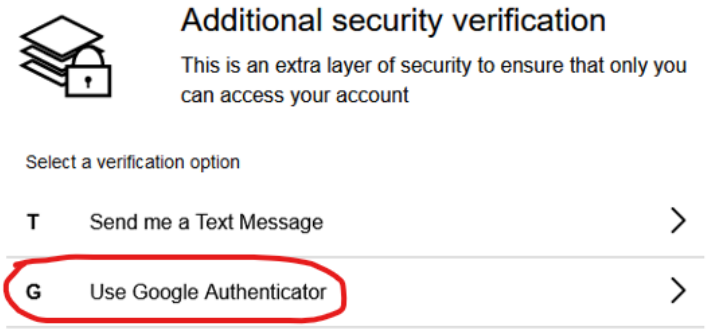
Enter this code on your screen and then click Register Google Authenticator.



Confirm that the registration was successful.



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



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.