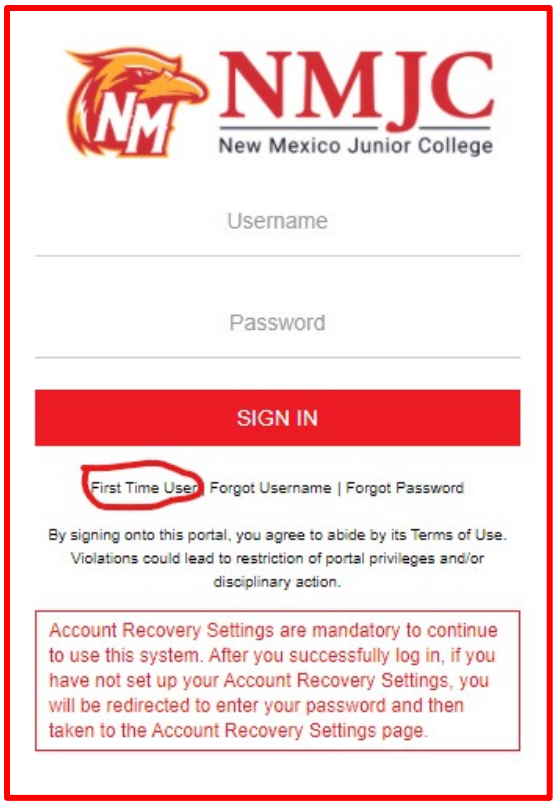
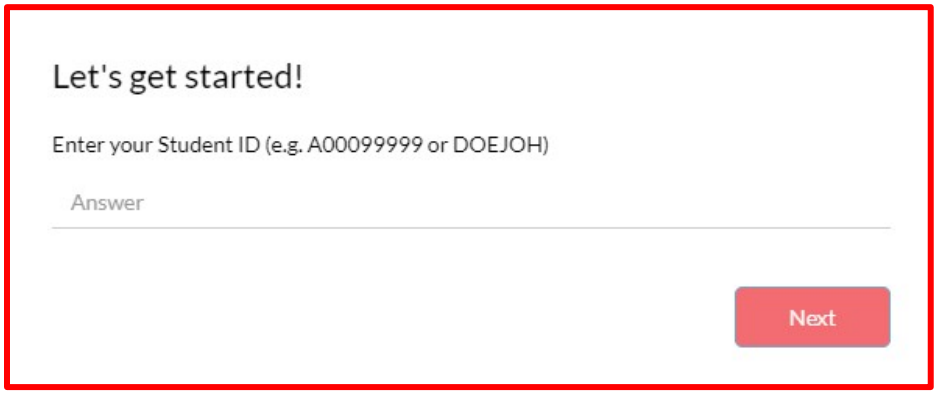
First Time User Setup

Follow the instructions below if this is your first time to log in to NMJC's Single Sign-On system, Quick Launch. You will need to know your Student ID, birth date, and the last 4 digits of your SSN to set up your account. This process will allow you to retrieve your User Name, which is now your NMJC Email account, and set your new password. This is the recommended process for all students because they would not know their Active Directory (Email) password and most do not know their NMJC Email Address. After a successful login, the system will force you to set up your account recovery options: security questions/answers, secondary email address, and phone number(s). This step is critical to ensure that you can recover your password on your own without any human intervention.

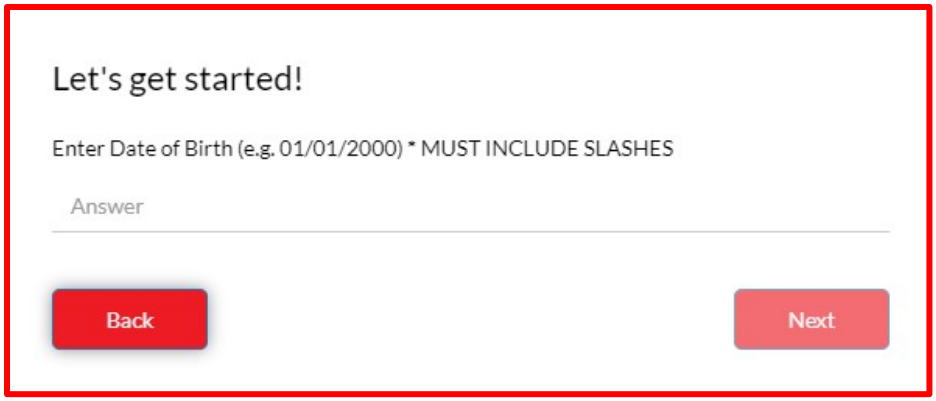
To access the system, please open a browser of your choice and go to https://sso.nmjc.edu. To get started, click on the First Time User link (see screenshot below).



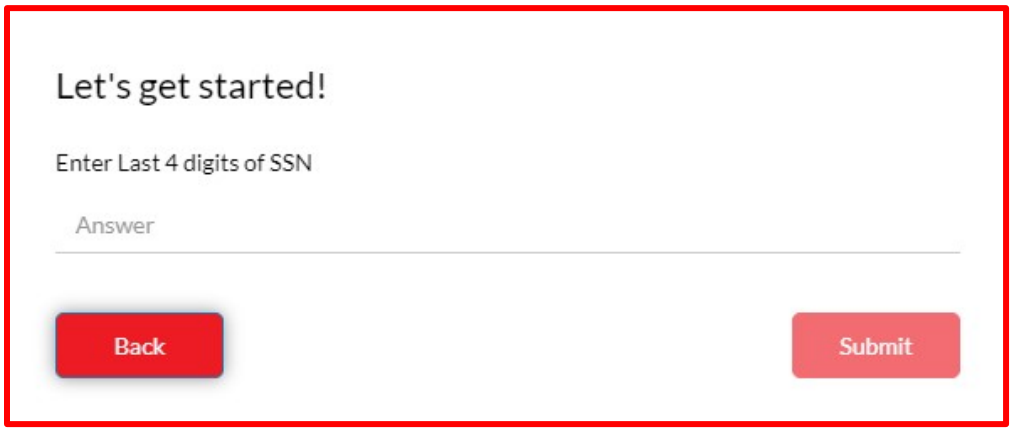
Enter your Student ID (e.g. A00099999) and then click Next.



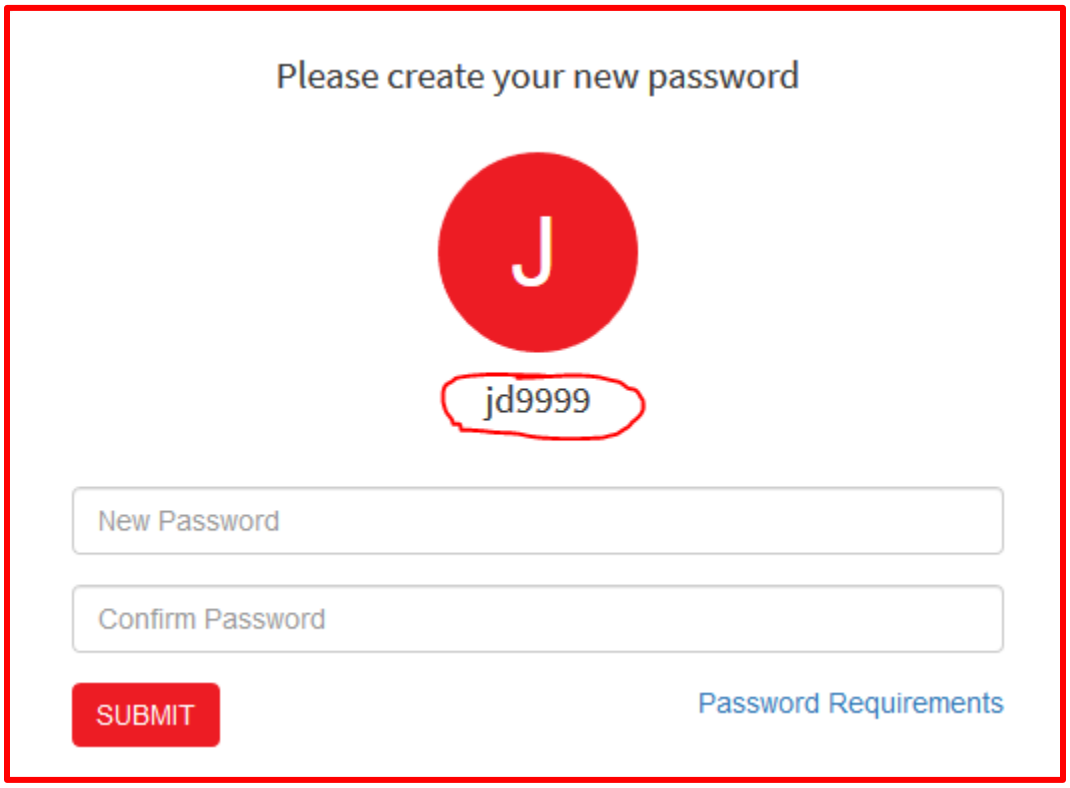
Enter your Date of Birth (include the slashes in the format MM/DD/YYYY) and then click Next.



Enter the last 4 digits of your SSN and then click Submit.



Please take note of your User Name (see screen shot below) as this will now be used to log into the system and then enter your new password (twice).



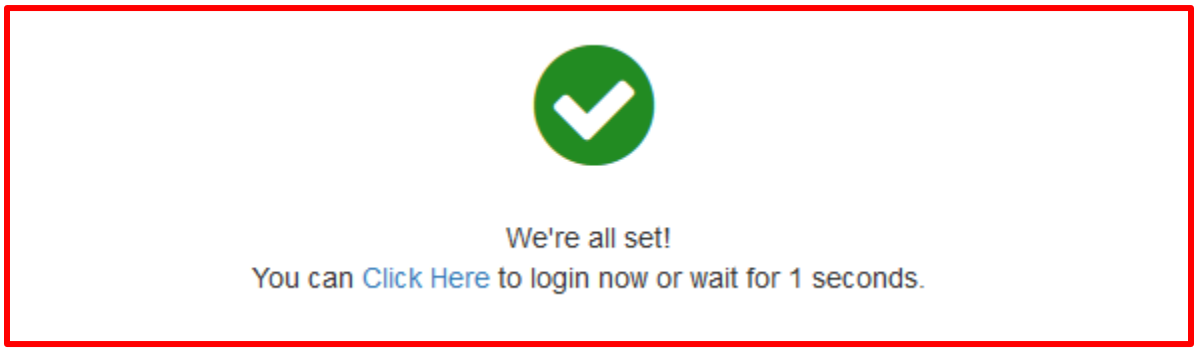
The password must:
Be at least 8 characters but not more than 14 characters

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be unique (cannot be one of your previous 5 passwords)

and contain characters from three of the following categories:

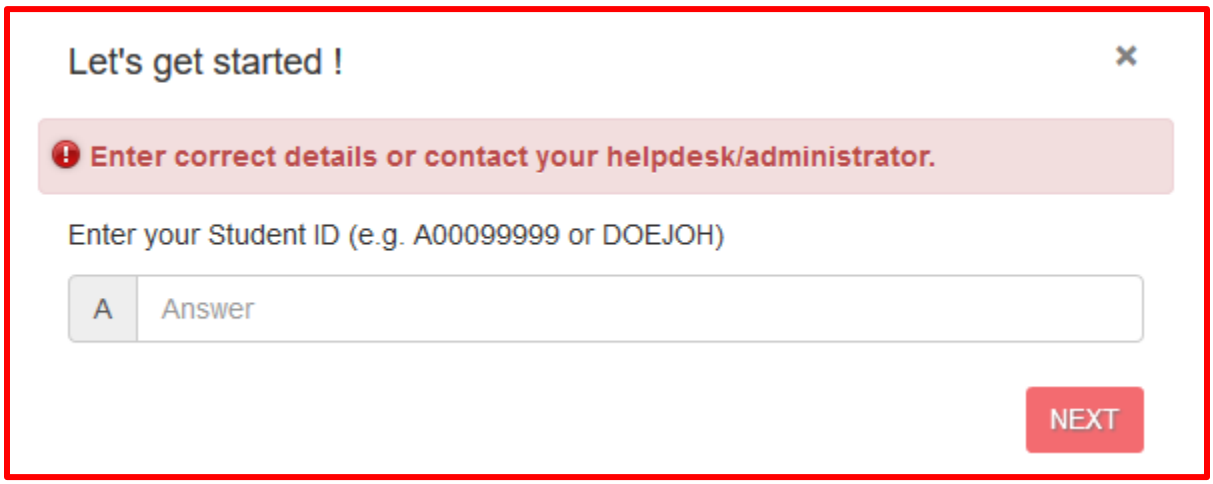
- Contain at least one uppercase letter (A through Z)
- Contain at least one lowercase character (a through z)
- Contain at least one digit (0 through 9)
- Contain at least one special character (for example, !, $, #, %)
- Contain any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

If you are successful, you will see the following message.

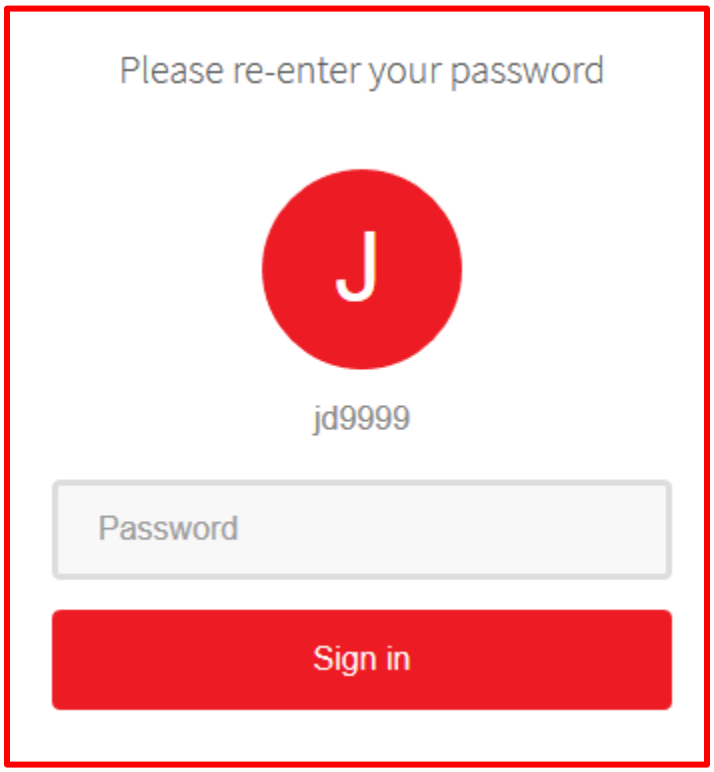


If you receive the following message below, make sure you are entering the correct information and in the correct format (if applicable). If you continue to have problems, please contact Computer Services.

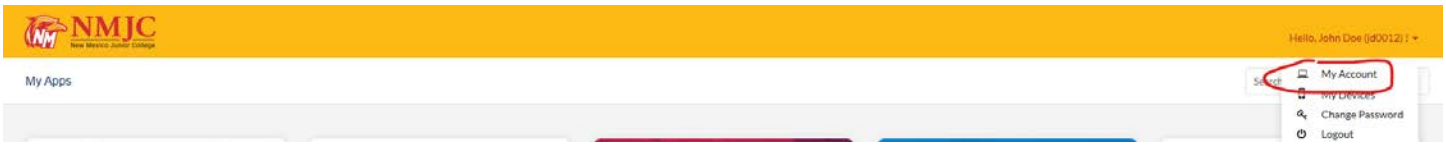
Employee Name	Phone	Email
Barbara Hicks	575.492.2500	bhicks@nmjc.edu
George Garcia, Jr.	575.492.2506	ggarcia@nmjc.edu
Jose Flores	575.492.2505	jflores@nmjc.edu
Bill Kunko	575.492.2501	bkunko@nmjc.edu



After a successful login, the system will force you to set up your account recovery options. The following message will appear and you must enter your current password to continue.

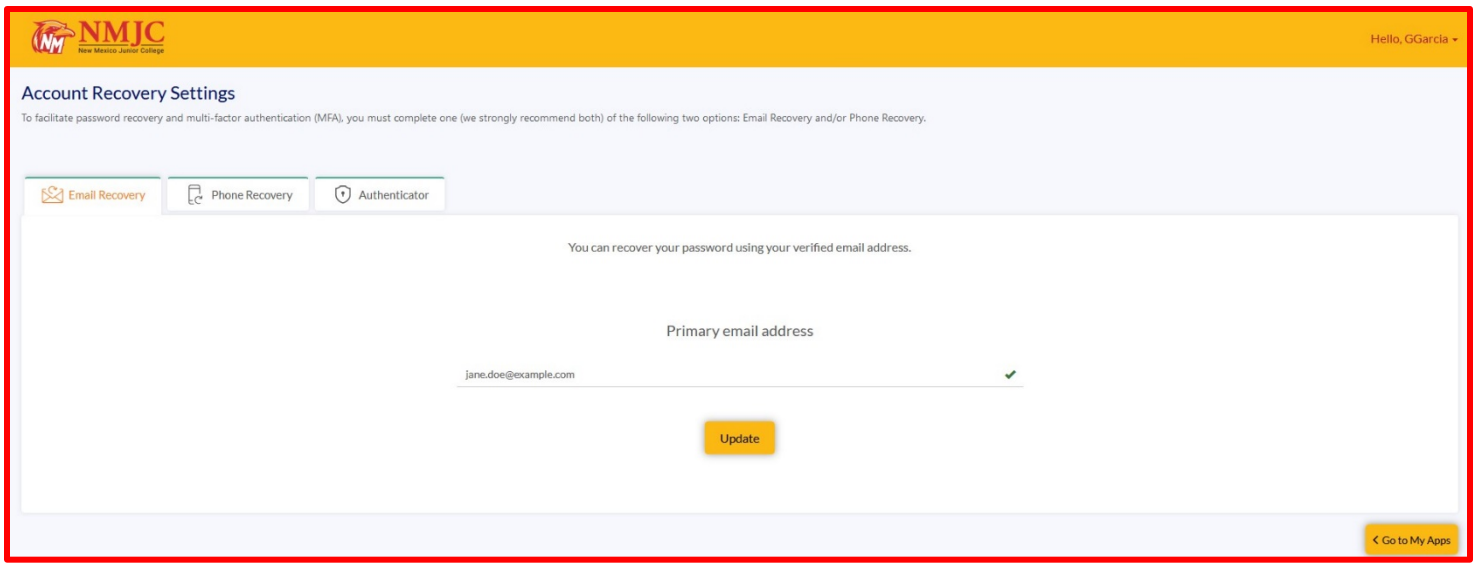


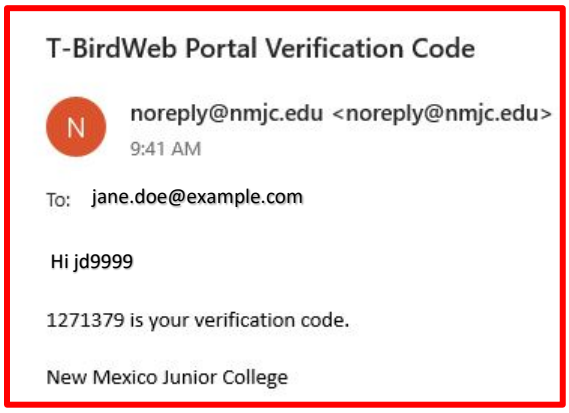
If you are not forced, you will still need to set up your account recovery options to utilize all the features of the system, which allows you to recover your account by accessing your secondary email address, allowing text messages to be sent to your primary or secondary cell phone number(s), or using Google Authenticator. You must set up at least one of these account recovery options to continue. We strongly suggest you set up all 3 options: secondary email, phone number(s), and security questions.

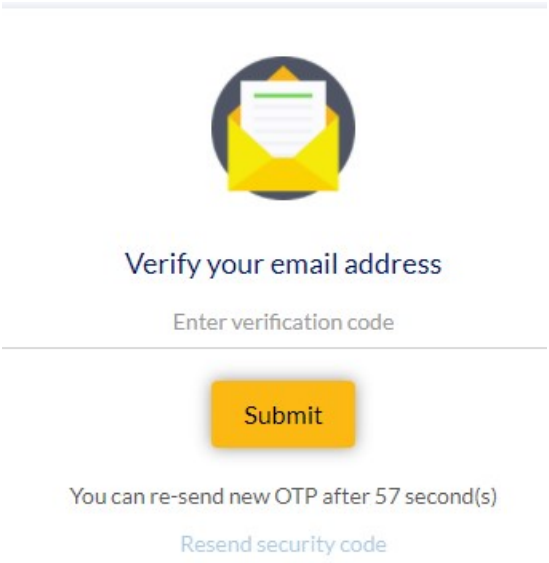


Please enter a secondary email address that you are able to access and that no one else is using. ***We DO NOT recommend that you use a family member's or friend's email address in this case as it needs to be unique in our system to work properly.*** The system will send an email to this address with a code to use to complete the setup. If you use this method to recover your password, you will need to be able to access this email account to retrieve the code to verify you. This is for your security. **If you did not receive the verification code in your Inbox, please check your Junk and/or SPAM folder(s).**

*** IMPORTANT: DO NOT USE YOUR NMJC EMAIL ADDRESS FOR YOUR SECONDARY EMAIL RECOVERY. YOU WILL NOT BE ABLE TO OBTAIN THE SECURITY CODE IF YOU CANNOT ACCESS YOUR NMJC EMAIL ACCOUNT.**

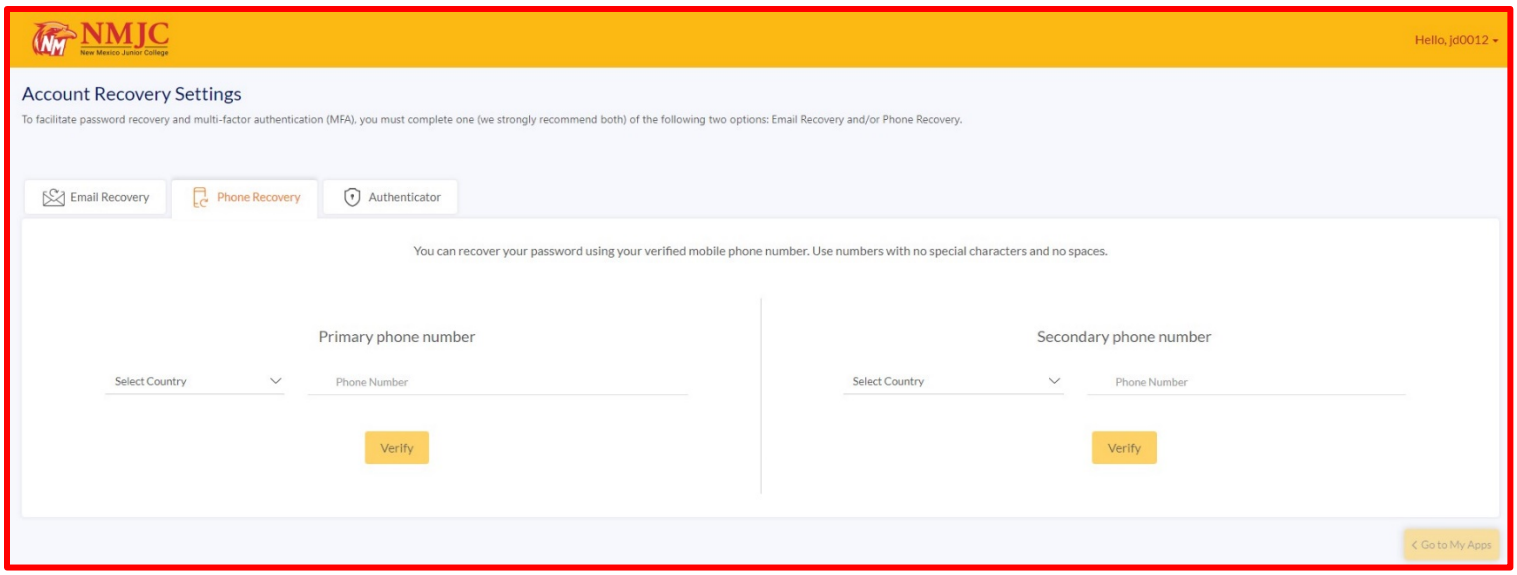


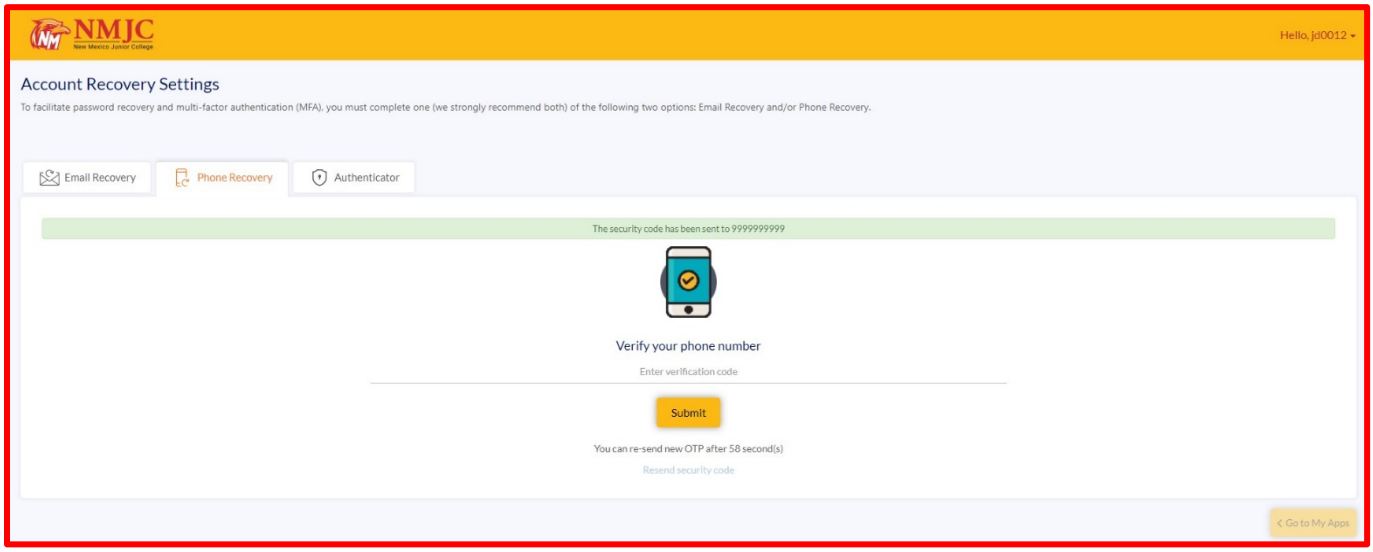


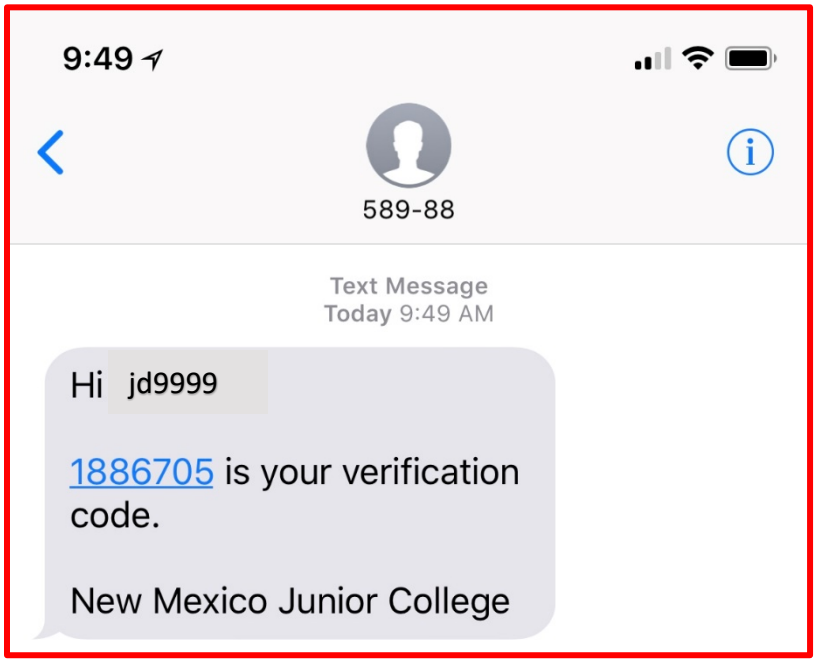


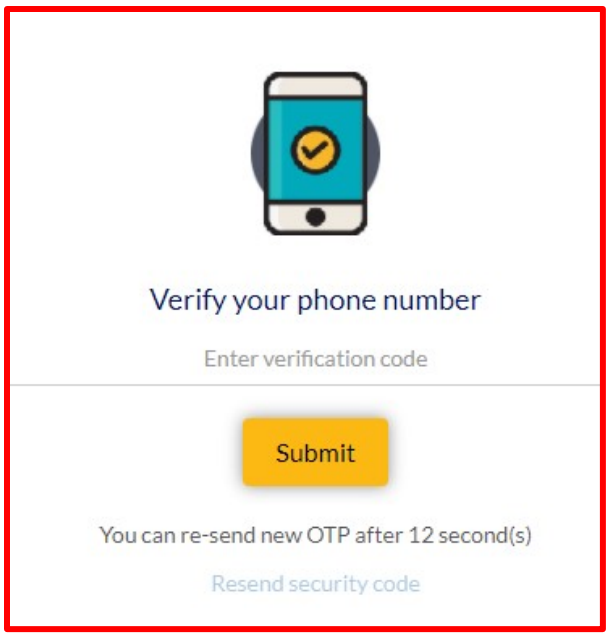
Please enter a primary and/or secondary cell phone number that you can access and will accept text messages. The system will send a text message to this phone number with a code to use to complete the setup. If you use this method to recover your password, you will need to be able to access cell phone numbers text message to retrieve the code to verify you. This is for your security.

*** IMPORTANT: Choose your country code first and then enter your phone number (including the area code first)**


NMJC
New Mexico Junior College
Hello, jd0012
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
You can recover your password using your verified mobile phone number. Use numbers with no special characters and no spaces.
Primary phone number
Select Country
Phone Number
Verify
Secondary phone number
Select Country
Phone Number
Verify
Go to My Apps


NMJC
New Mexico Junior College
Hello, jd0012
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
The security code has been sent to 9999999999
Verify your phone number
Enter verification code
Submit
You can re-send new OTP after 58 second(s)
Resend security code
Go to My Apps


9:49
589-88
Text Message
Today 9:49 AM
Hi jd9999
1886705 is your verification code.
New Mexico Junior College



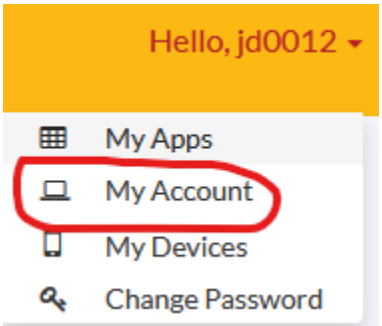
Google Authenticator is a software-based authenticator by Google that implements two-step verification services using the Time-based One-time Password Algorithm (TOTP; specified in RFC 6238) and HMAC-based One-time Password algorithm (HOTP; specified in RFC 4226), for authenticating users of software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

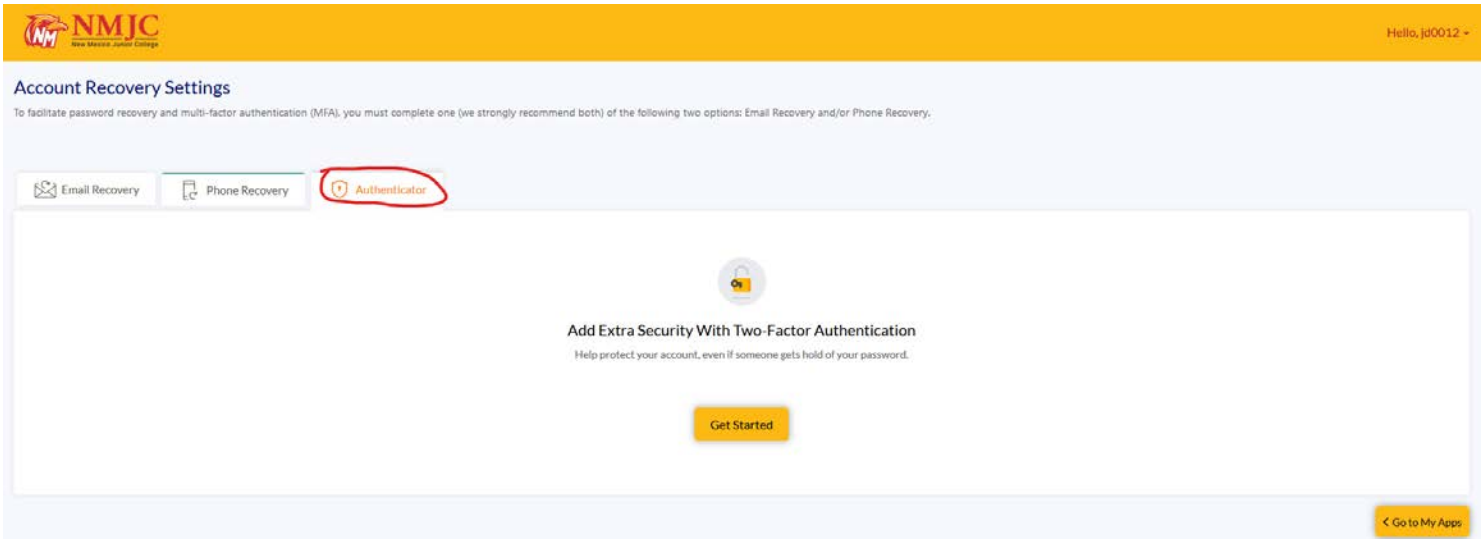
How to set up Google Authenticator in the T-BirdWeb Portal?

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

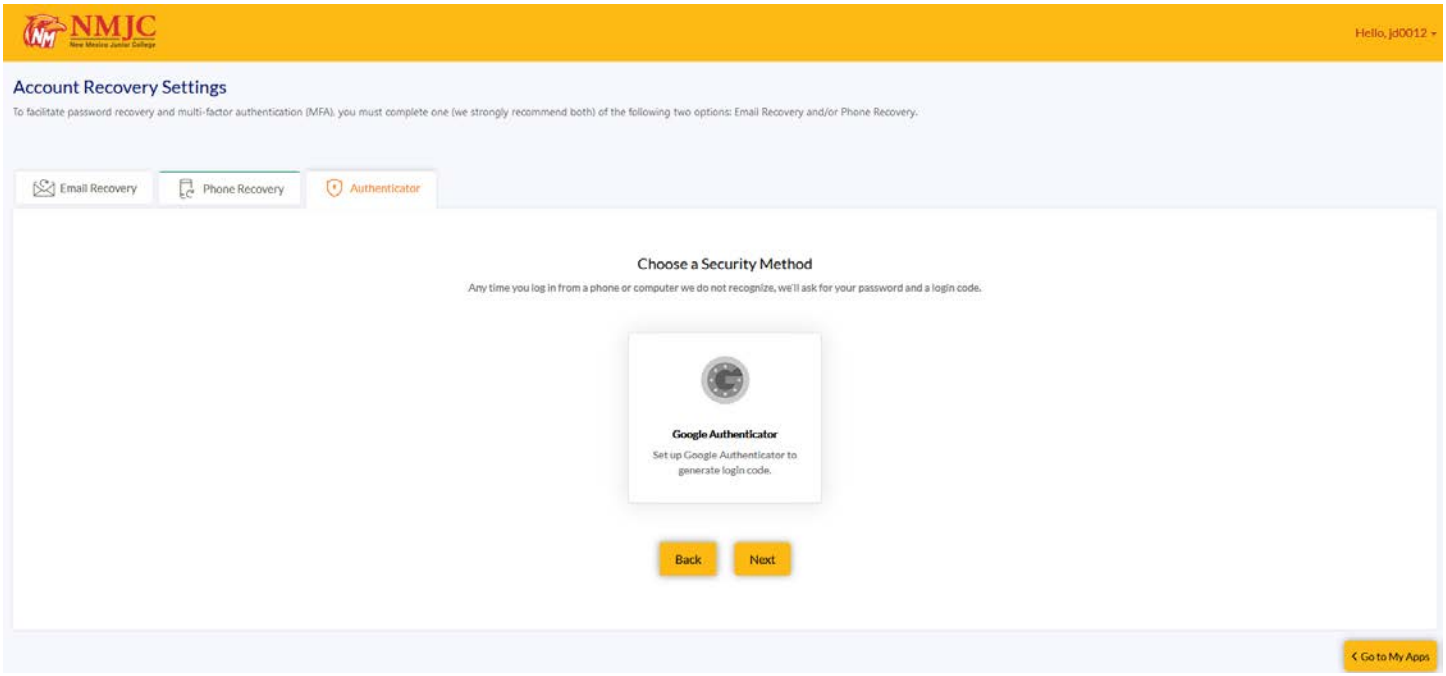
Using a device other than the device where the Google Authenticator app is installed, log in to the T-BirdWeb Portal, click the drop-down menu located to the right of your Username, then click My Account and enter your password if prompted.



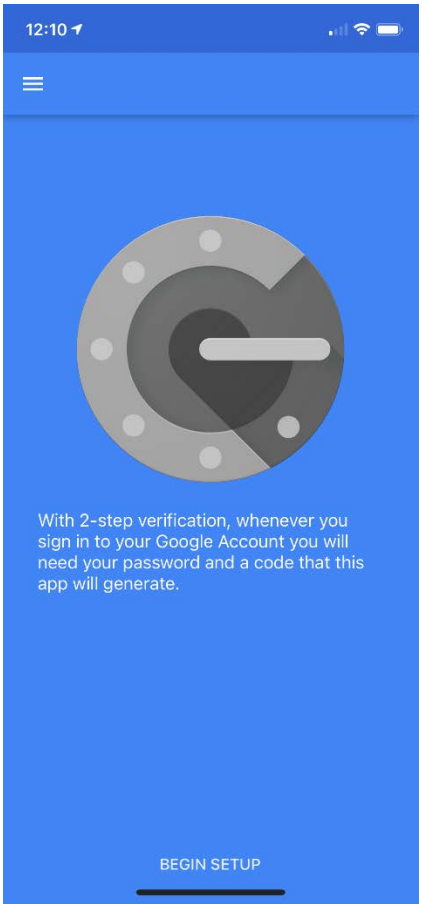
Click on the Authenticator tab. Click on Get Started.



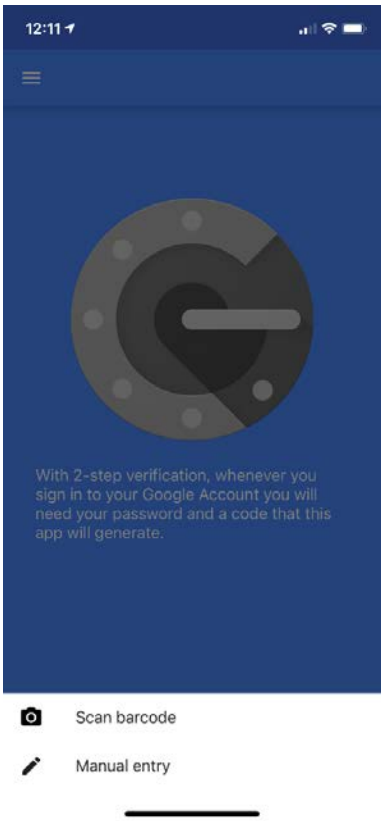
Click Next.



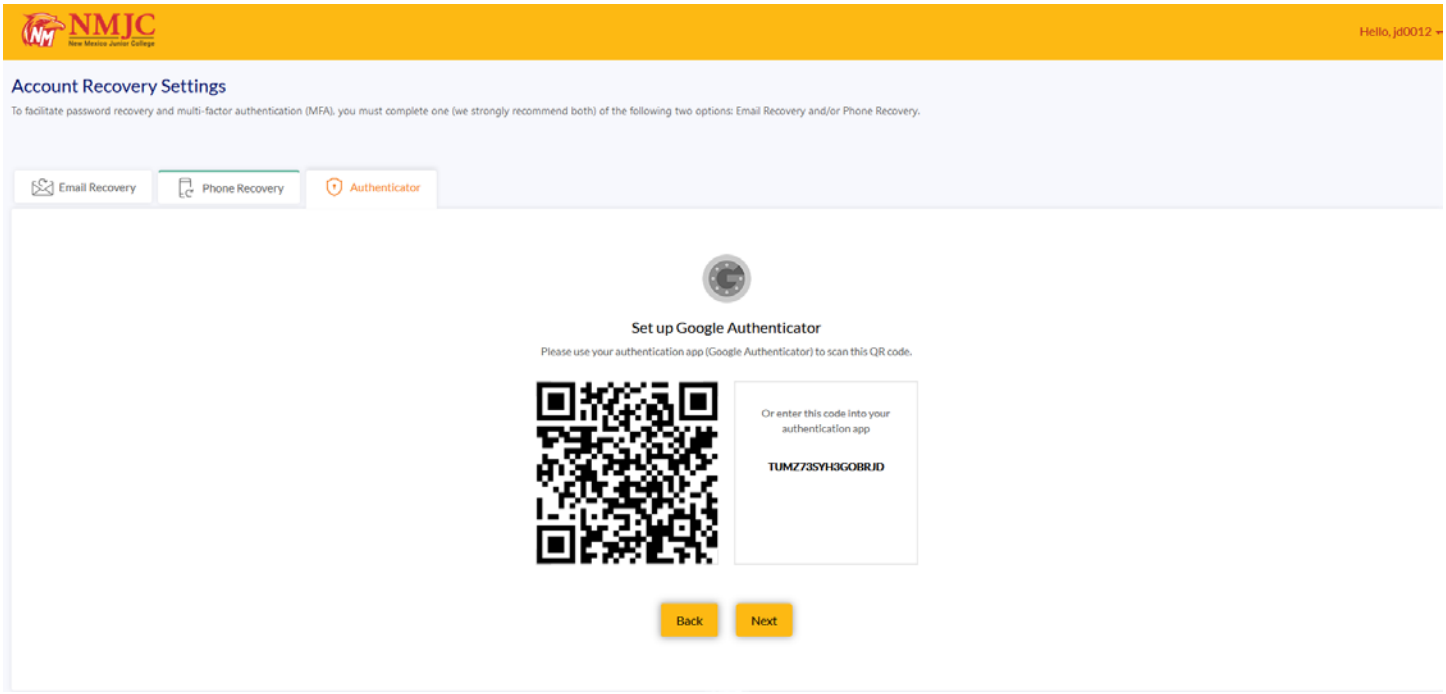
Open the Google Authenticator app on your mobile device and tap Begin Setup.



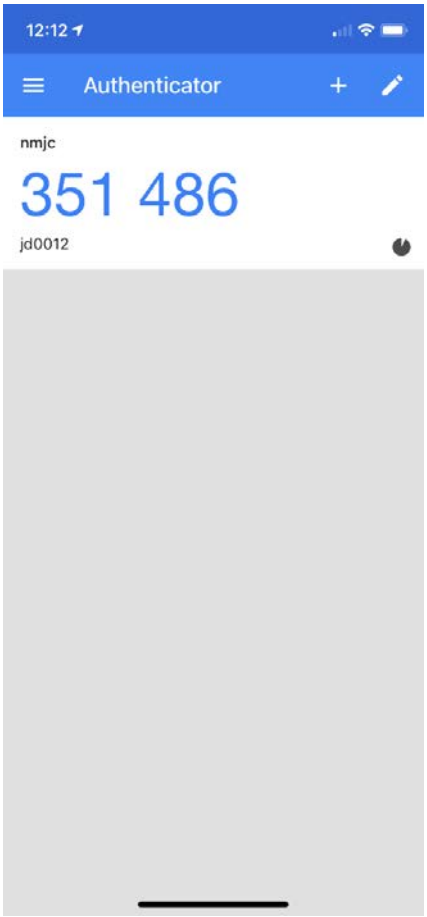
Tap Scar barcode.



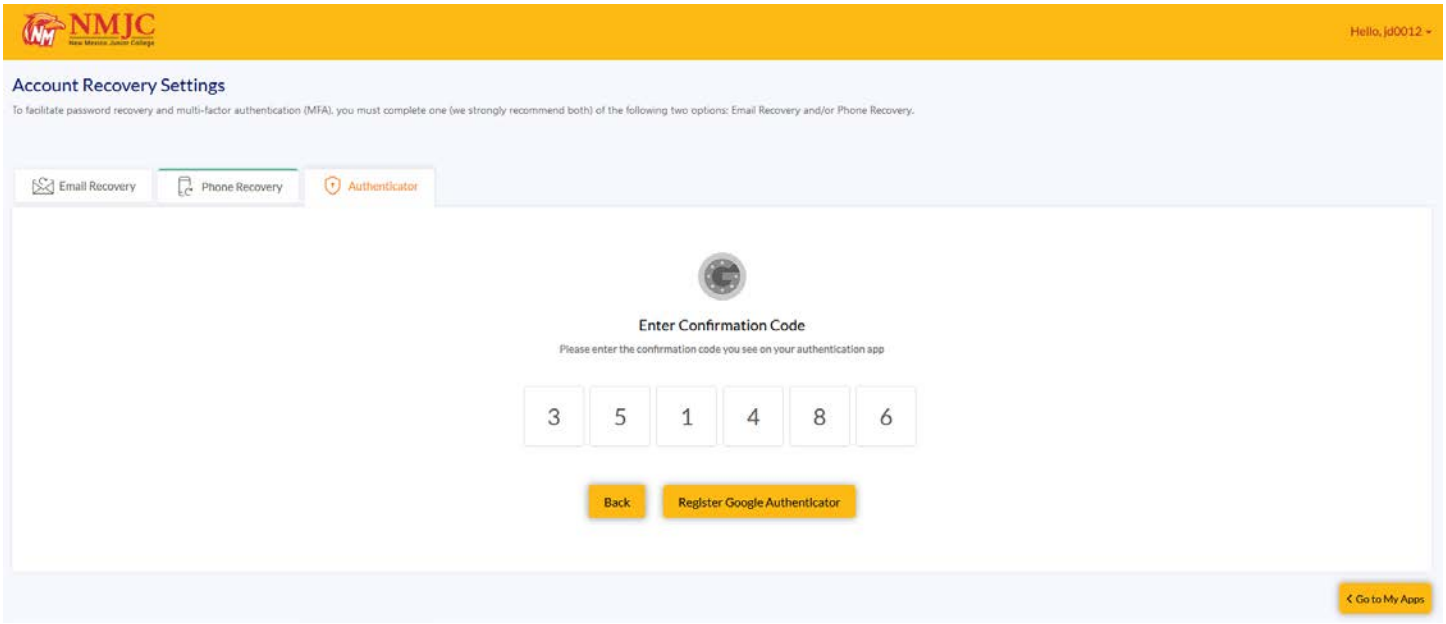
Point your mobile device’s camera at the QR code on the screen.



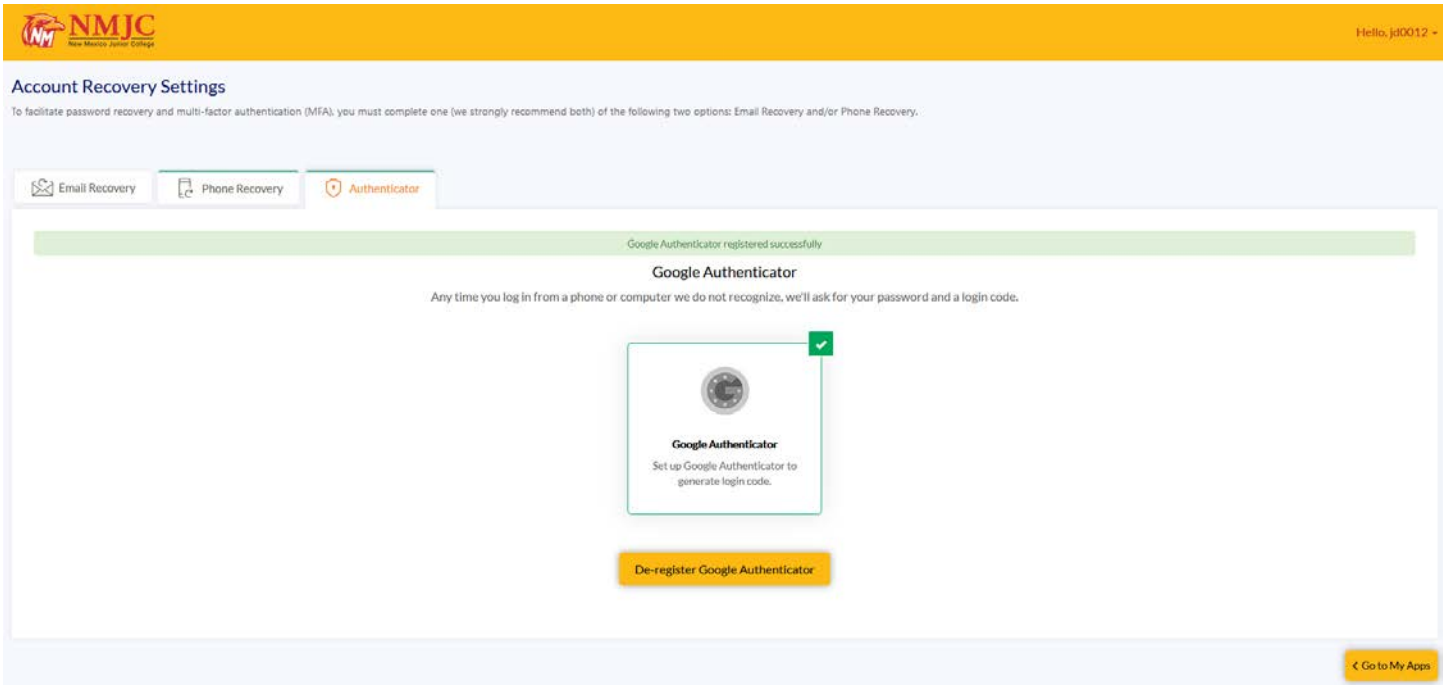
If successful, your app will look like this.



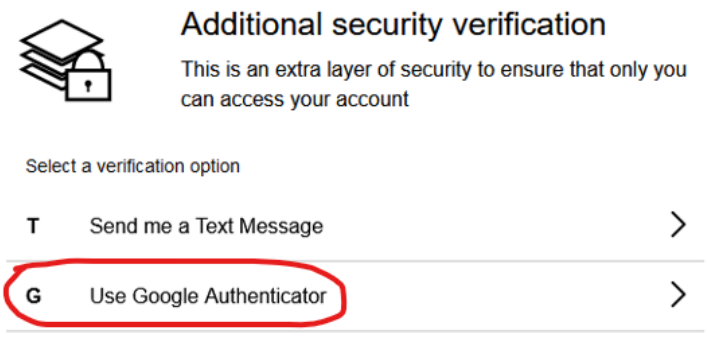
Enter this code on your screen and then click Register Google Authenticator.



Confirm that the registration was successful.

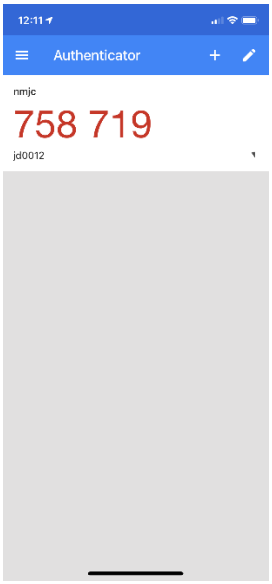


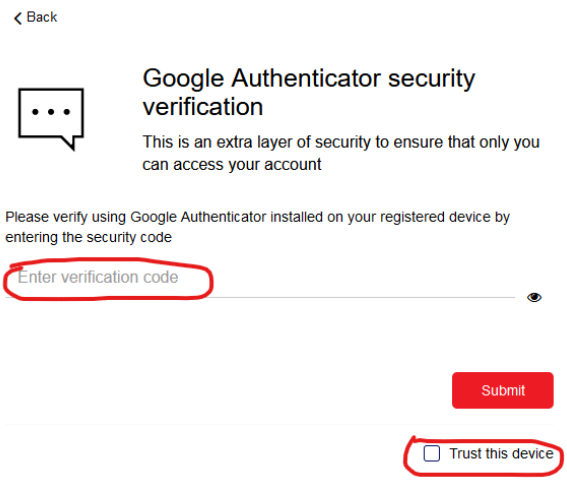
Now, when you log in to the T-BirdWeb Portal or request a password reset, you will have this choice.



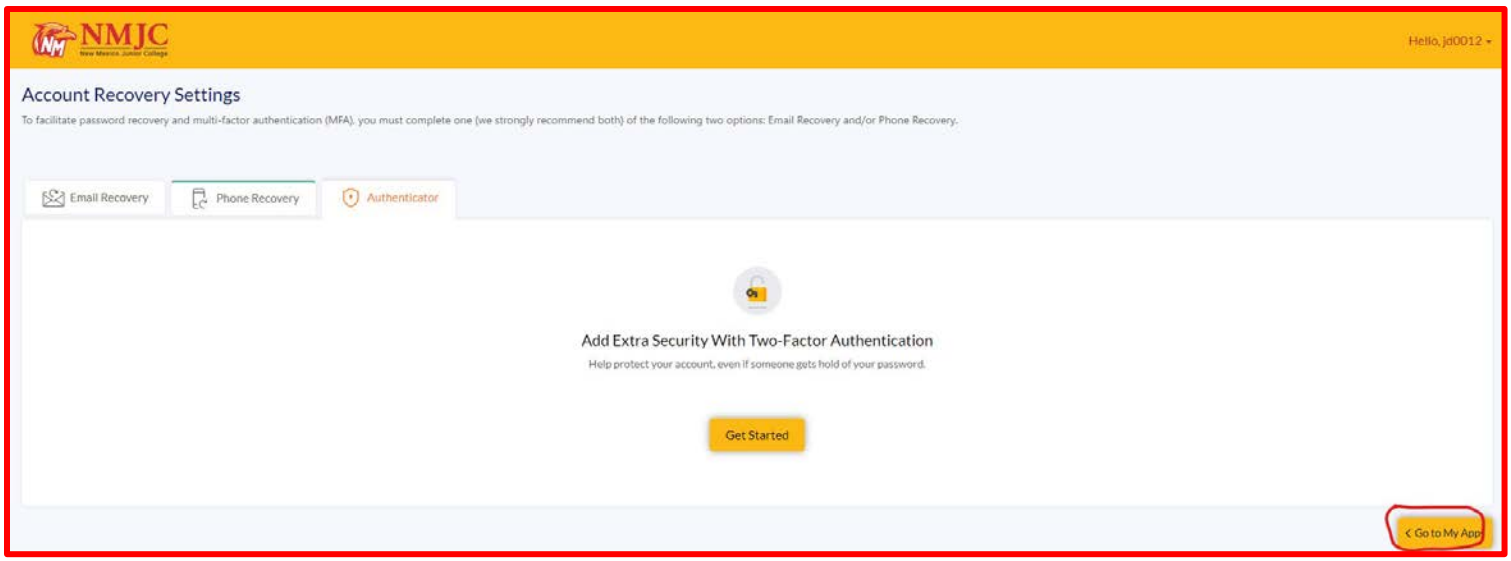
Open the Google Authenticator app on your phone and enter the code. If you are using a device that you trust, make sure you check the ***Trust this device*** checkbox before you click the Submit button.

Note: The code will change often.





When you are finished, please click the Go to My Apps button to return to the Dashboard.



You can always update this information or change your password at any time by going into the My Account or Change Password link.