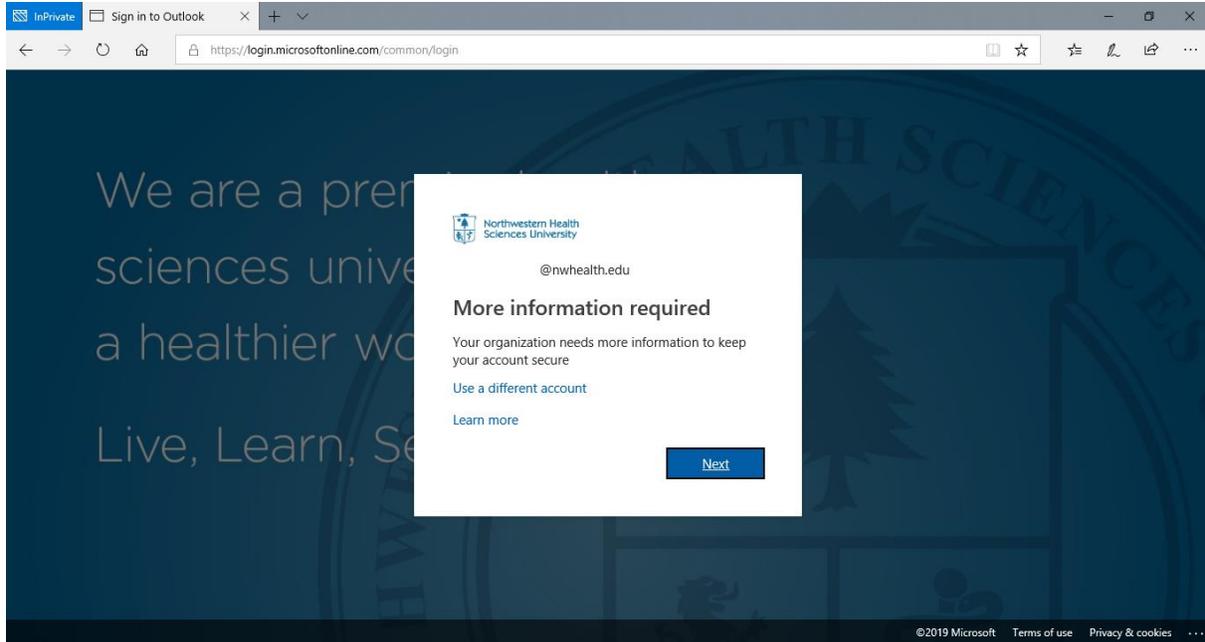


How to Configure Multi-Factor Authentication at NWHSU

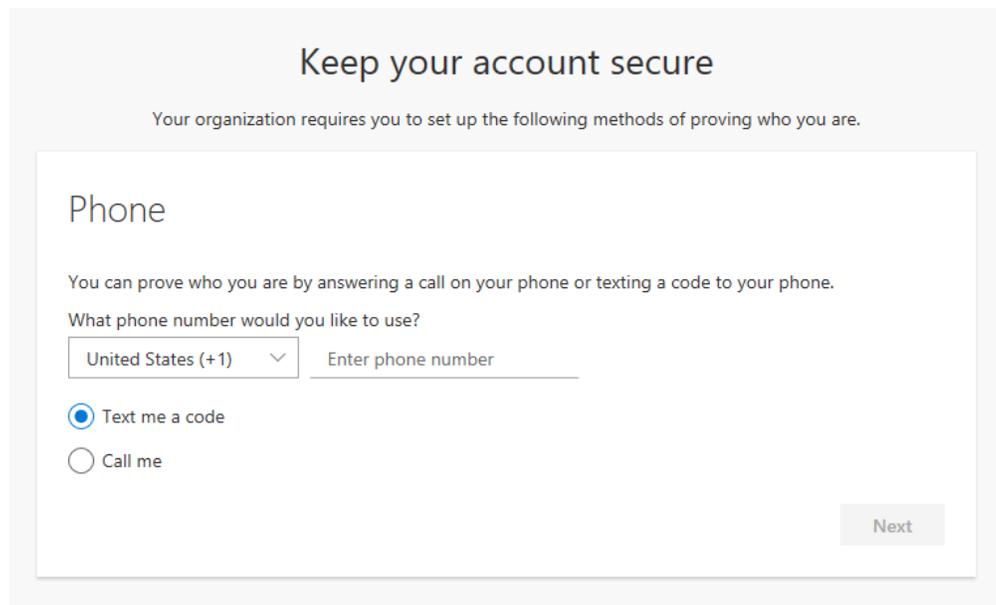
Using your telephone to verify your identity:

The first time you log into your school email account (<https://mail.nwhealth.edu>) from off-campus, you will see a notification that more information is required in order to login. The notification will normally appear as follows:

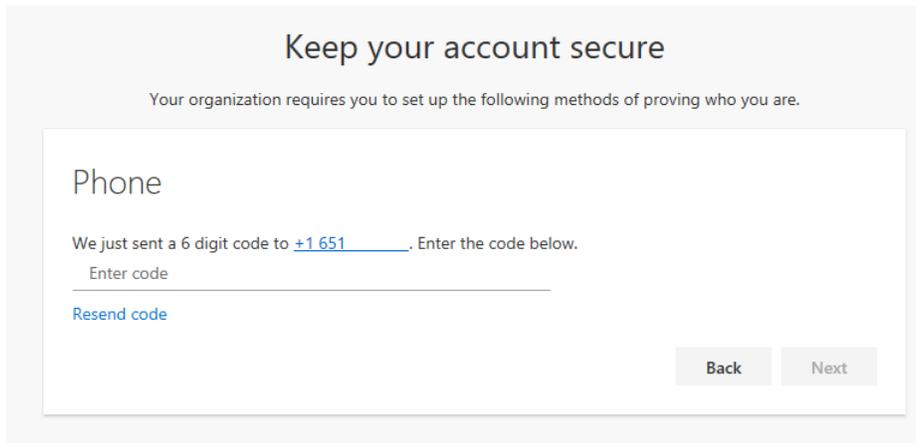


Please click “Next” when the notification appears.

After clicking “Next,” you will be prompted to enter a phone number as an additional MFA identity. Select your preferred method of registering your phone number, either by text or an automated phone call. The phone number must be a mobile phone if you wish to receive text messages for authenticating your identity.

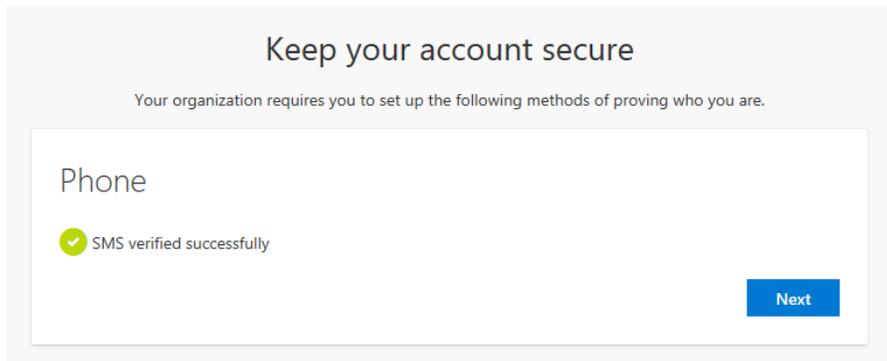


After entering your phone number, a 6-digit code will be provided either via text message or automated phone call. Enter the code in the dialog that will look like this:

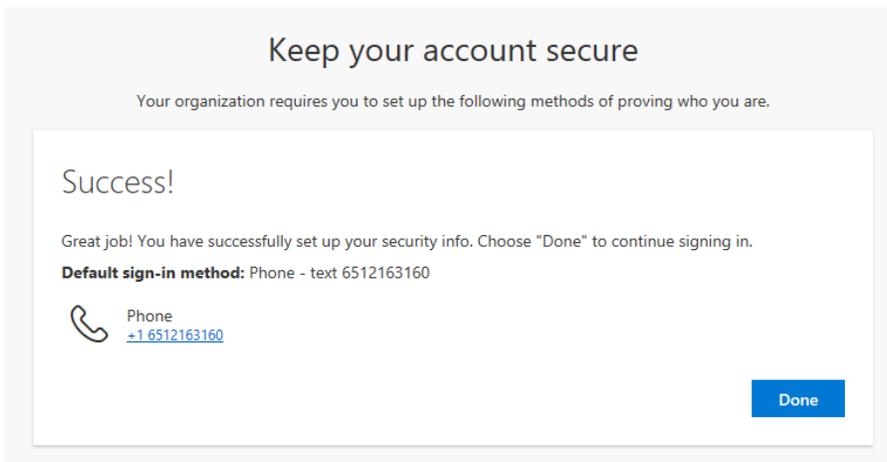


The screenshot shows a dialog box titled "Keep your account secure" with the subtitle "Your organization requires you to set up the following methods of proving who you are." The main heading is "Phone". Below it, the text reads: "We just sent a 6 digit code to +1 651 _____. Enter the code below." There is an input field with the placeholder text "Enter code" and a "Resend code" link below it. At the bottom right, there are two buttons: "Back" and "Next".

Your phone number will now be registered after you enter the code and can be used as a MFA identity confirmation. You then see the following two dialogs. Click "Next" and then "Done". **Note:** The phone number can also be used to reset your password by clicking on the Forgot my Password link when trying to sign in.



The screenshot shows a dialog box titled "Keep your account secure" with the subtitle "Your organization requires you to set up the following methods of proving who you are." The main heading is "Phone". Below it, there is a green checkmark icon followed by the text "SMS verified successfully". At the bottom right, there is a blue button labeled "Next".



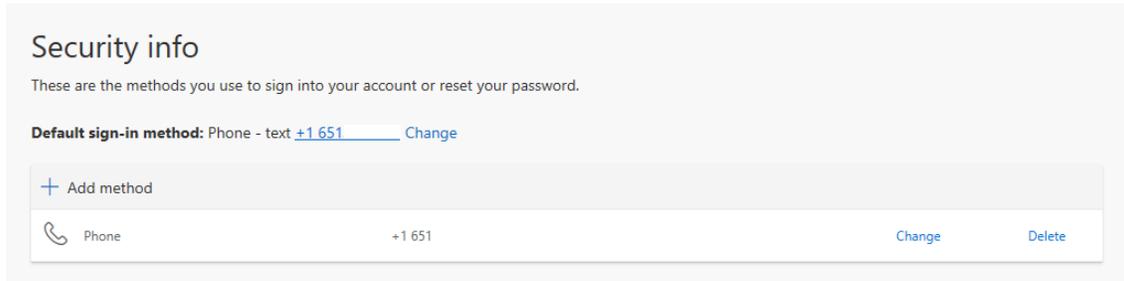
The screenshot shows a dialog box titled "Keep your account secure" with the subtitle "Your organization requires you to set up the following methods of proving who you are." The main heading is "Success!". Below it, the text reads: "Great job! You have successfully set up your security info. Choose 'Done' to continue signing in." There is a line of text: "Default sign-in method: Phone - text 6512163160". Below this, there is a phone icon followed by the text "Phone" and a blue link "+1.6512163160". At the bottom right, there is a blue button labeled "Done".

Using the Microsoft Authenticator App to verify your identity:

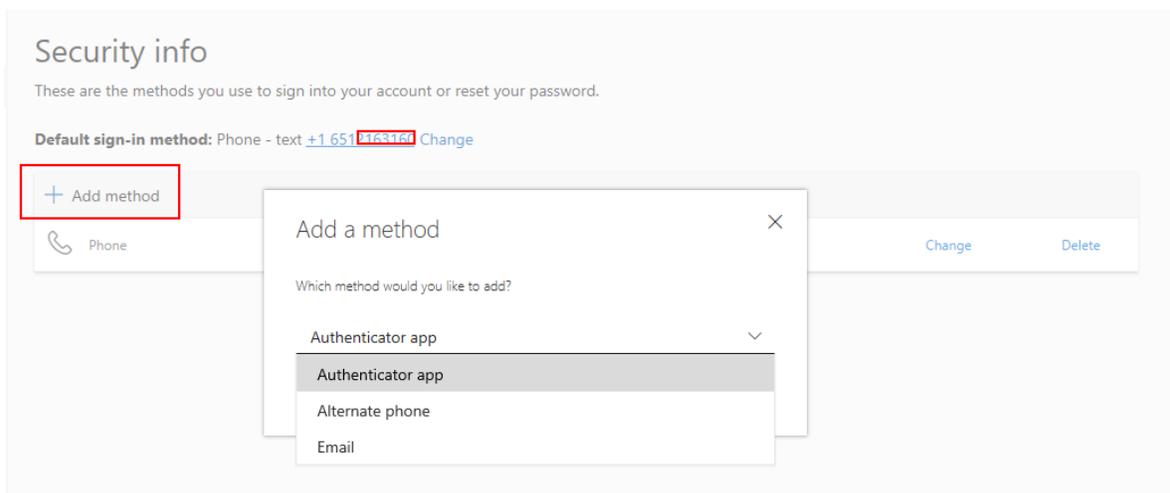
The preferred MFA identity method is an authenticator app on your smart phone. You may download the Microsoft Authenticator app from either the Apple App Store or Google Play Store. To setup the authenticator app, download and install the app from the appropriate store.

On your computer and after the app is installed go to <https://aka.ms/mfasetup>.

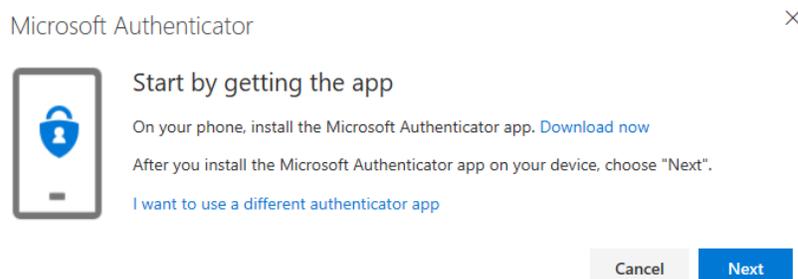
You will be prompted to sign in and you will see your current list of MFA identities. If you just setup MFA using a phone number, this list will only include your phone number.



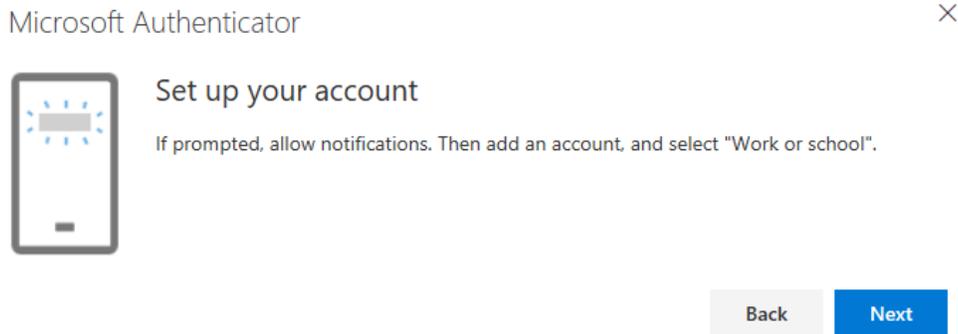
Click the Add Method link and select Authenticator App.



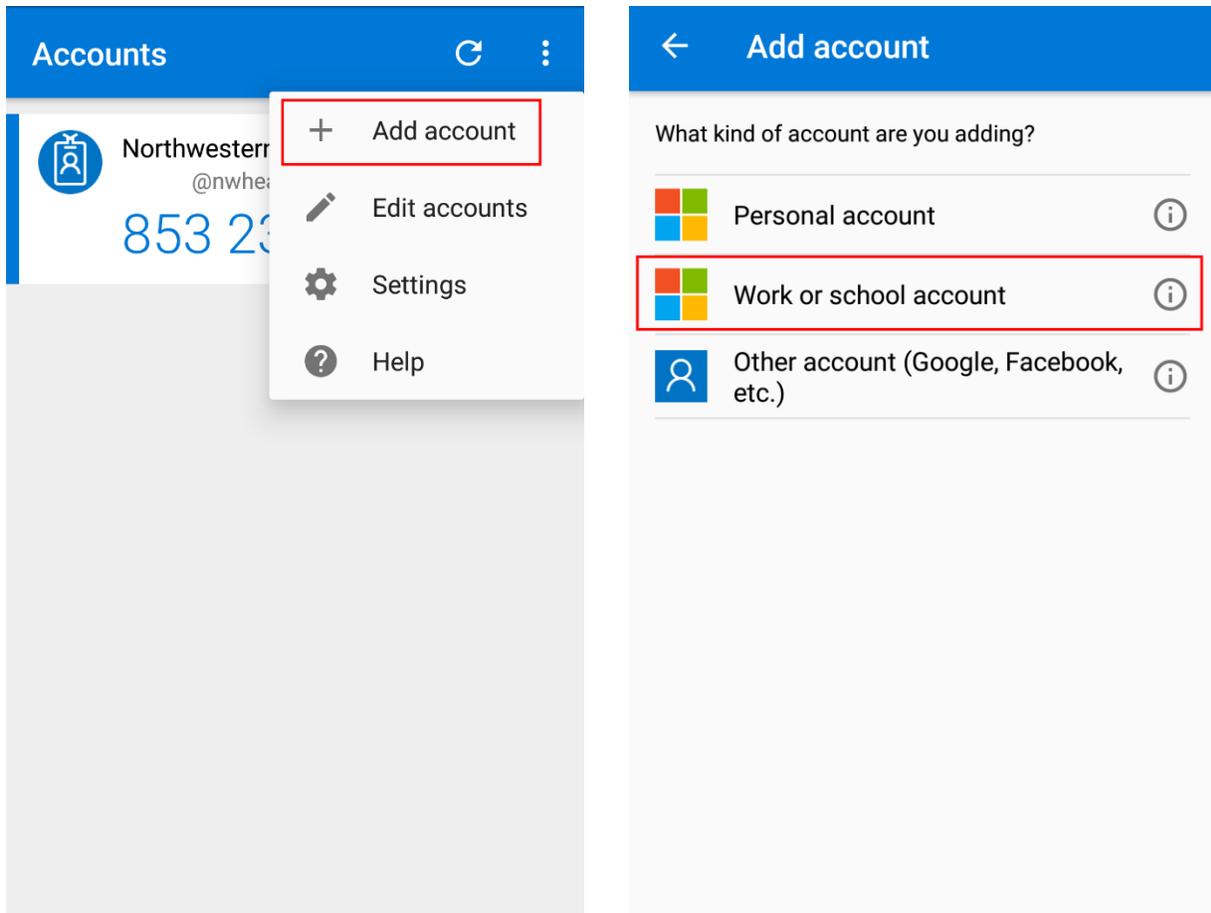
You will now see the following on your computer's screen. Click "Next" since you have already install the authenticator app:



You should now see the following on your computer's screen. Click "Next" on this dialog as well.



Open the authenticator app, tap the ellipsis button at the upper right, click Add Account, and select Work or School Account.



On your computer, scan the QR code with your phone as shown in the image below. If you can't scan the QR code, click the "Can't scan image" link and put the Code and URL into the authenticator app.



Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

[Can't scan image?](#)

Back

Next



Scan the QR code

Use the app to scan the QR code below. This will pair the app with your account.



Cancel

Next

[Can't scan the QR code?](#)

Enter the following info into your app:

Code:
284402

URL:
<https://bn1pfpad08.phonefactor.net/pad/542680>

A notification will appear prompting you to approve an authentication request. Approve the request when it appears.

If everything above is successful, you will get a message saying the app has been approved as a MFA identity.



✔ Notification approved

Back

Done

Set the Microsoft Authenticator application as the default MFA Identity Verification:

Finally, we recommend changing the default MFA identity from phone number, to the authenticator app.

To do this, go to go to <https://aka.ms/mfasetup>.

After signing in, click "Change" next to the Default sign-in method as show in the image below.

Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Phone - text +1 651 [Change](#)

+ Add method			
	Phone	+1 651	Change Delete
	Microsoft Authenticator		Delete

Select the authenticator app from the drop down as shown.

Change default method ✕

Which method would you like to use to sign in?

Microsoft Authenticator - notification ▼

[Back](#) [Confirm](#)

After selecting the authenticator app, you will see a message stating that the default sign-in method was updated.

Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Microsoft Authenticator - notification [Change](#)

+ Add method			
	Phone	+1 651	Change Delete
	Microsoft Authenticator		Delete

Your default sign-in method was updated ✕