NEW YORK STATE | Office for People With Developmental Disabilities

CHOICES Cloud Logon Process and Multi-Factor Authentication MFA Set Up Guide

May 6, 2025

Last Revision: June 2026

Table of Contents

Logon Process and Multi Factor Authentication (MFA) Requirement 3
1. Microsoft B2B and Invitation acceptance 3
1.1 Non-Microsoft Agency Users 4
1.2 MFA - SMS Text Instructions 7
1.3 Microsoft 365 SSO Users 10
2. MFA - MS Authenticator Instructions 11
2.1 MFA – MS Authenticator pre-installed 14
3. Updating MFA Settings 17

Current External Users as of June 2025 - Logon Process and Multi Factor Authentication (MFA) Requirement

All external users whose current ***username*** begins *Public*\, will use their agency email address as their ***username*** to logon to CHOICES as of June 16th migration to the Cloud.

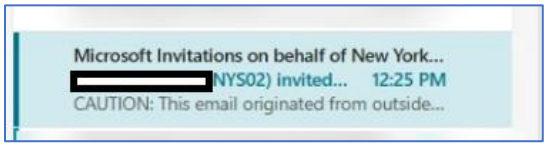
Example of ***Username*** - **my.name@myagency.org.**

All external users will be required to set up and use multi-factor authentication (MFA) to logon to CHOICES once migrated to the Cloud. Please check with your CCO or Agency regarding the option of MFA to use.

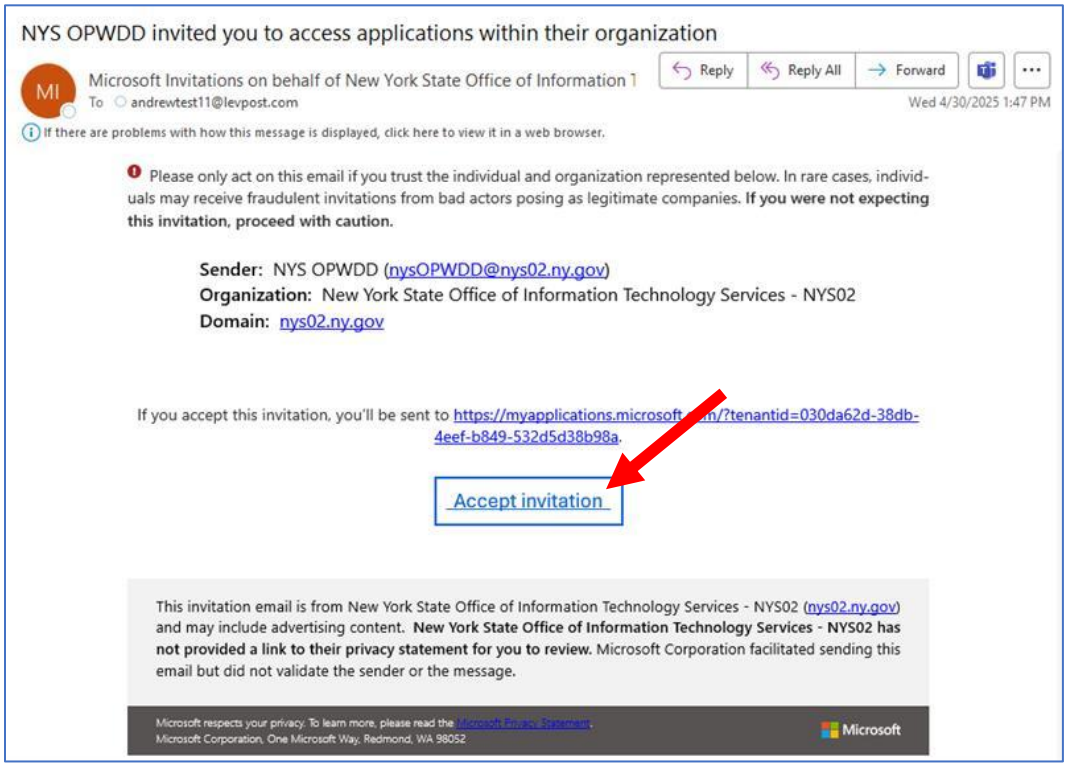
1. Microsoft B2B and Invitation acceptance

Prior to any user logging into CHOICES Cloud version, all users will receive an invitation from Microsoft on behalf of NYS Information Technology Services (ITS) & OPWDD to verify the user's email by accepting the invitation. This is a one-time verification for all users' CHOICES accounts.

The graphic below shows how the email will display in the user's Inbox



Below is a graphic of the Email body in reading pane. The user must click "Accept invitation" to begin the verification process and move to the logon.



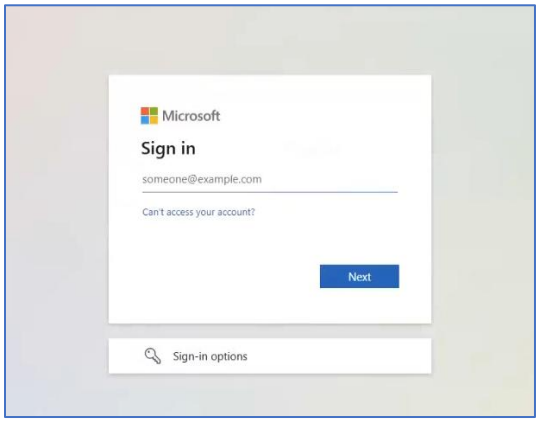
At this point the user experience will be one of two paths. If your agency has Microsoft 365 Single Sign On (SSO) see Section 1.3 or if your agency does not have Microsoft 365 SSO see Section 1.1.

NYS OPWDD (State) staff go to Section 1.3 to begin the logon process. State staff are not required to add MFA.

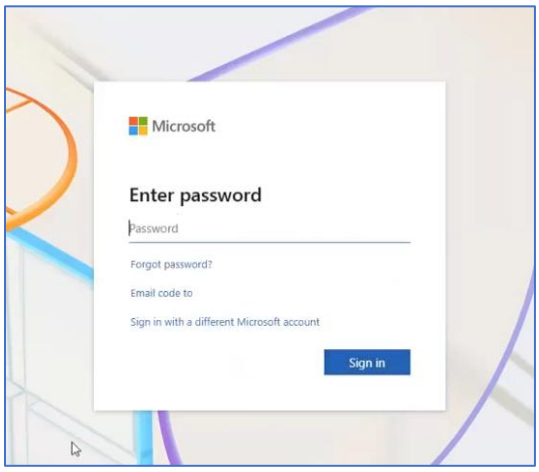
1.1 Non-Microsoft Agency Users

A new window will display to begin the logon process.

Enter your email

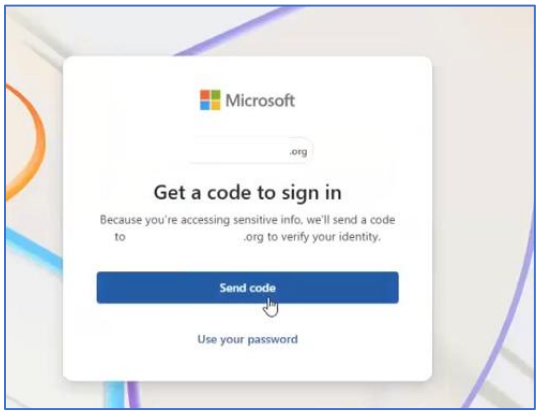


Enter your agency email password

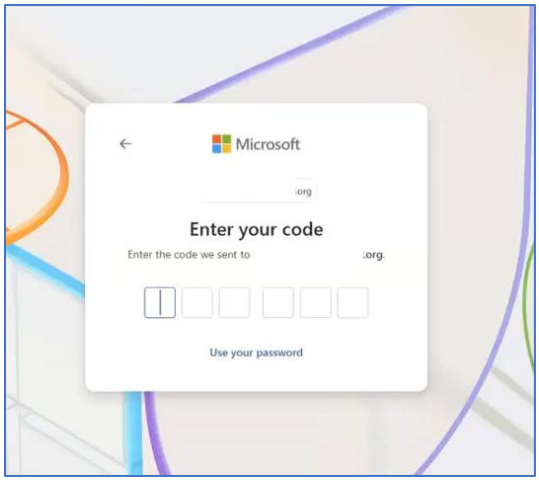


The non-Microsoft user will see *one* of the following two popups requesting the user get and enter a *one-time* passcode to verify their email address for the B2B security protocol.

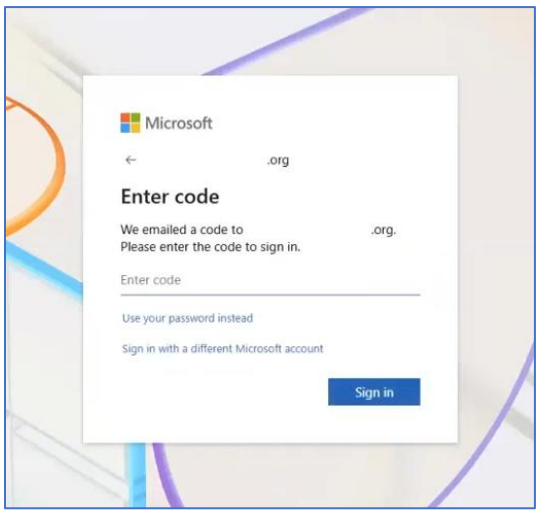
Option A) The user will first need to request a code to be sent. Click on “Send code”



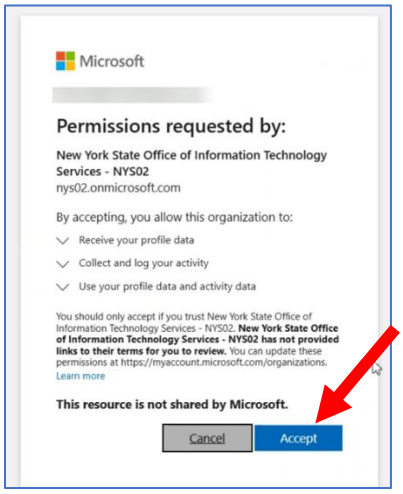
The user will need to check their email, copy the code to enter it into the popup. Popups may vary in look and or style.



Or Option B) the user may get this popup stating the user was emailed a code and to enter it here.

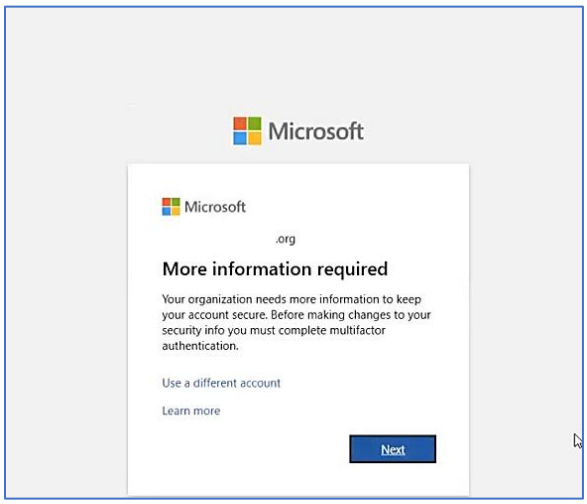


Next a popup will display noting the permissions being requested by NYS ITS while the user is logged into CHOICES. Click Accept.



This completes the one-time verification process.

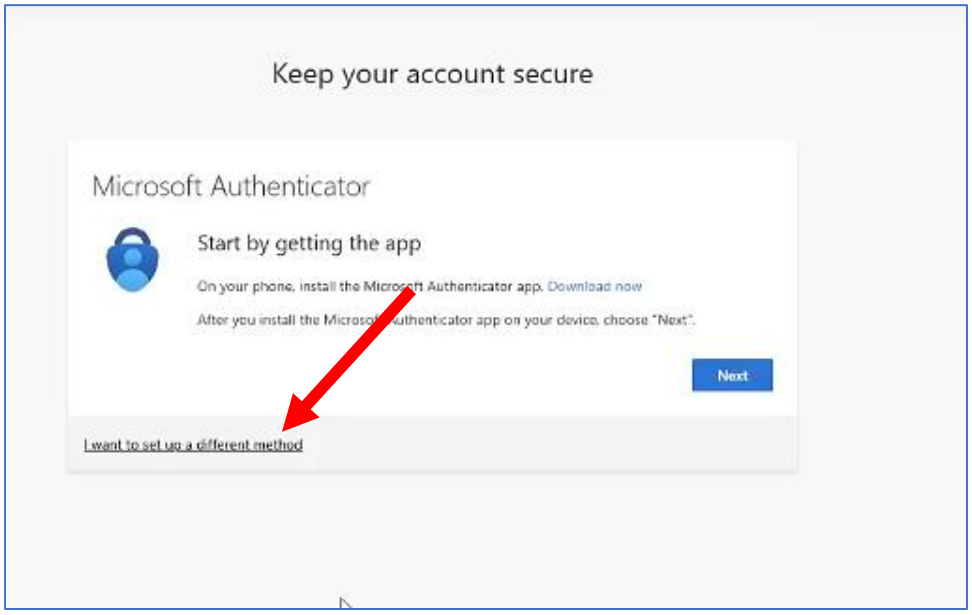
Next the external user will be requested to set up MFA. Click Next.



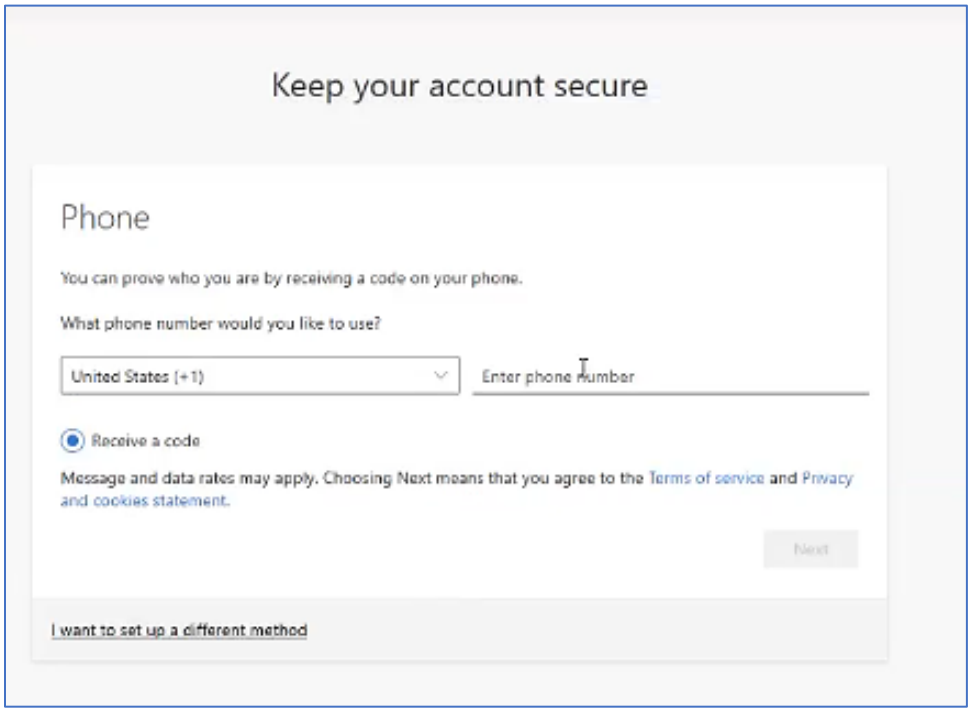
If the user is selecting the MFA option of SMS text continue to follow the instructions here. But if the user is selecting the MS Authenticator app, please go to Section 2 for instructions.

1.2 MFA - SMS Text Instructions

At this popup, click “I want to set up a different method”

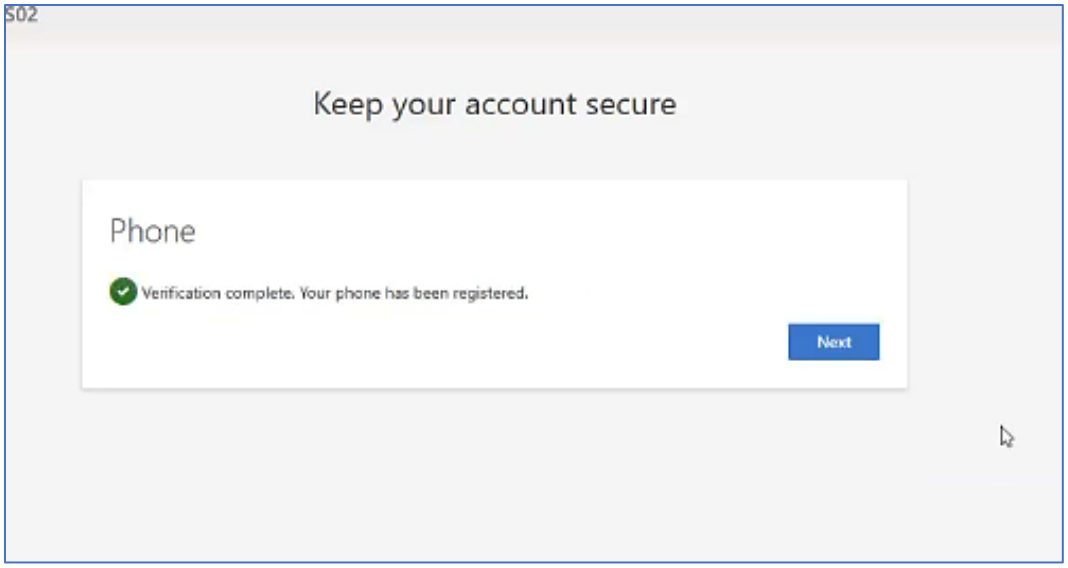


At this popup check that the option, Receive a code, is selected and then enter your phone number. This must be a smartphone that will allow text messages.

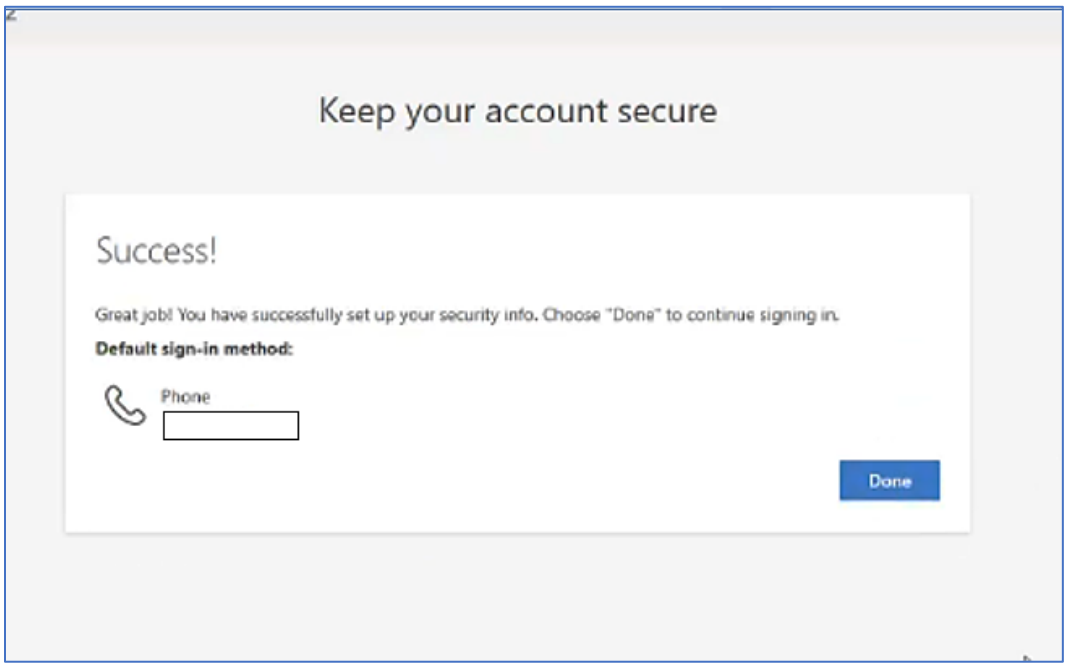


Enter the text sent to your phone. Once the text is entered the Next button will be available. Click Next.

The user is notified that the phone is registered for the SMS text MFA option. Click Next

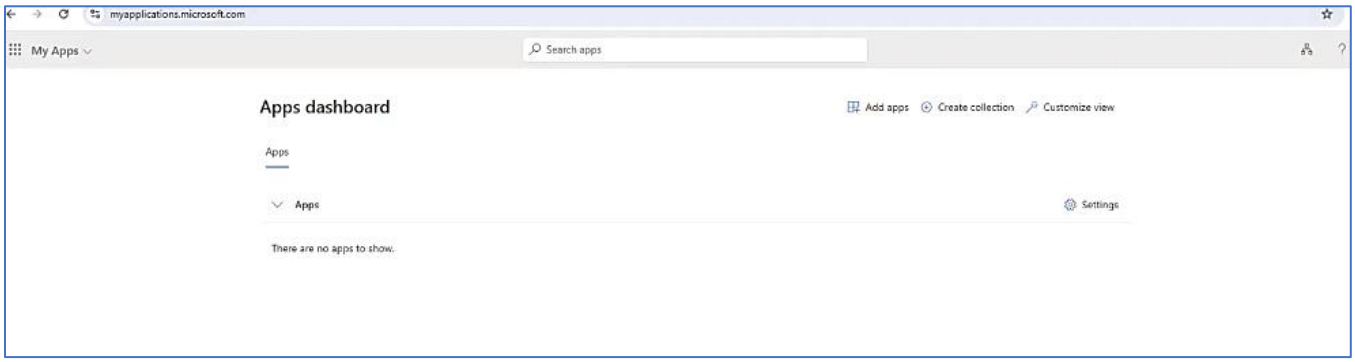


Then click Done.



This will complete the *initial* user account set up process and the user will be brought to the Apps dashboard page.

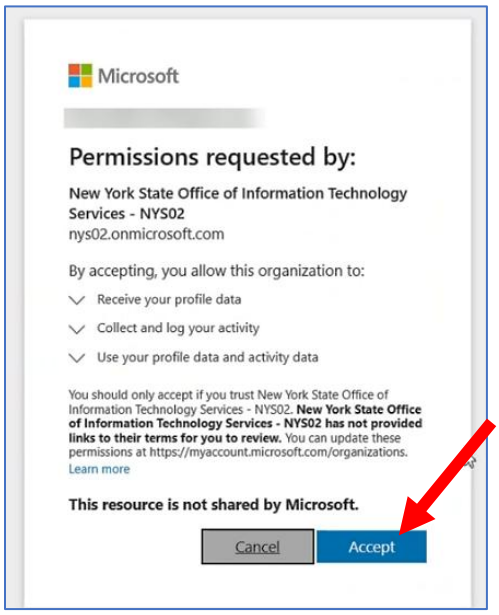
Once CHOICES has been migrated to the Cloud, users will be brought to the CHOICES application.



1.3 Microsoft 365 SSO Users

Once the user has accepted the B2B invite, the following the popup will display. The permissions being requested by NYS ITS are regarding when the user is logged into CHOICES.

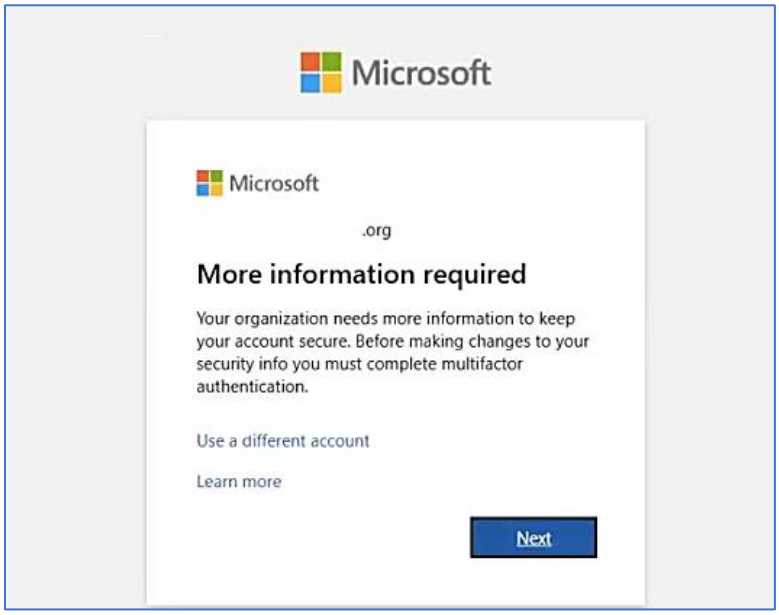
Click Accept.



This completes the one-time verification process.

Next the external user will see the following popup requesting more information to set up MFA.

Click Next.



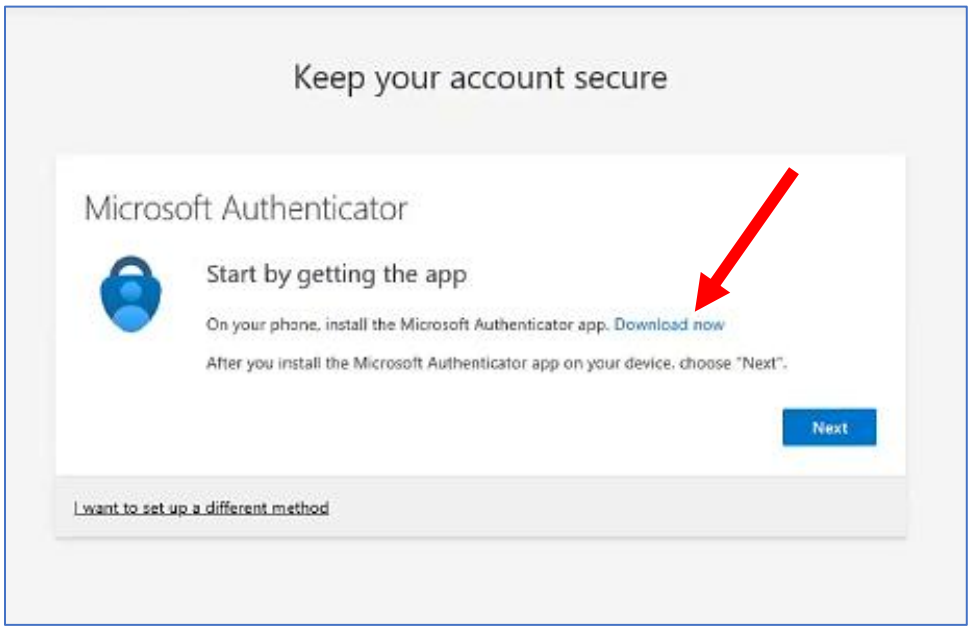
2. MFA - MS Authenticator Instructions

At this screen the default is for the user to set up the Microsoft Authenticator app.

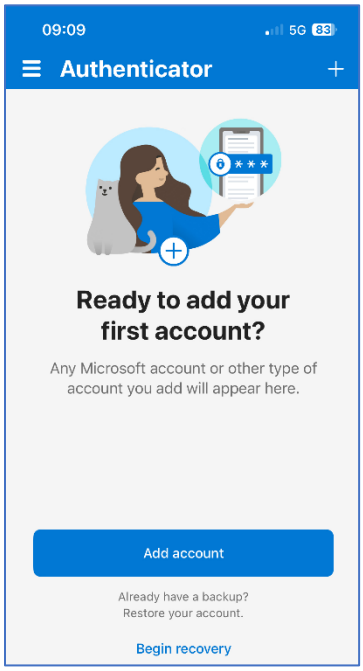
If the user already has the Authenticator app on their phone, skip ahead to Section 2.1, MFA – MS Authenticator App Pre-installed.

If the users *does not* yet have the MS Authenticator app downloaded to their phone, click the link, Download now

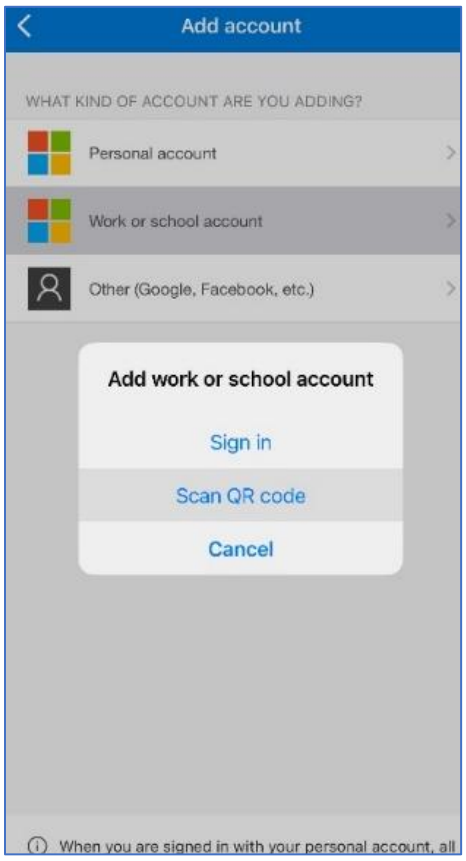
Please follow the instructions to download either the Android or IOS based on your phone's system.



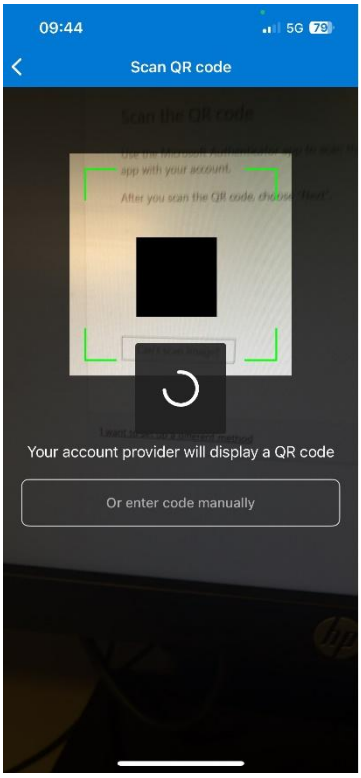
For users who have just downloaded the app, open the app and follow the steps till the prompt, Add account, is displayed. The following screen shots will vary depending on your phone.



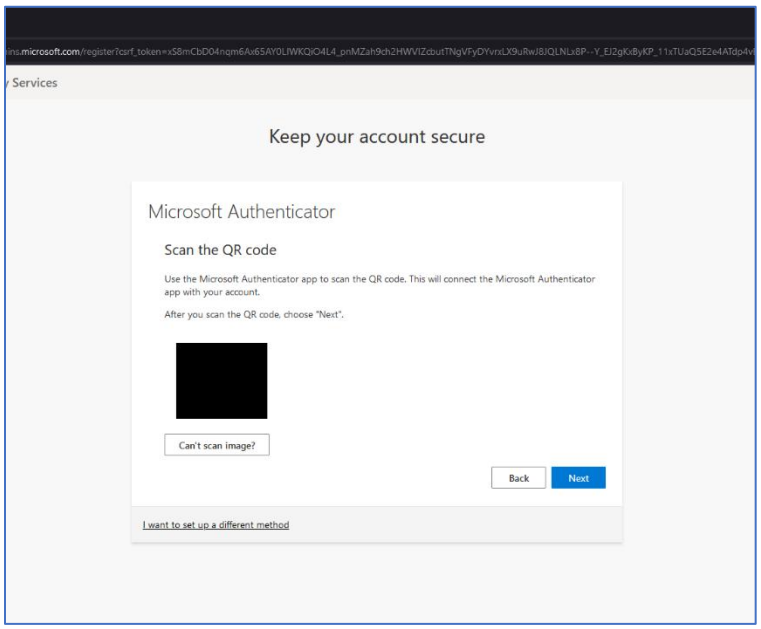
Select Work or School account, then select Scan QR code



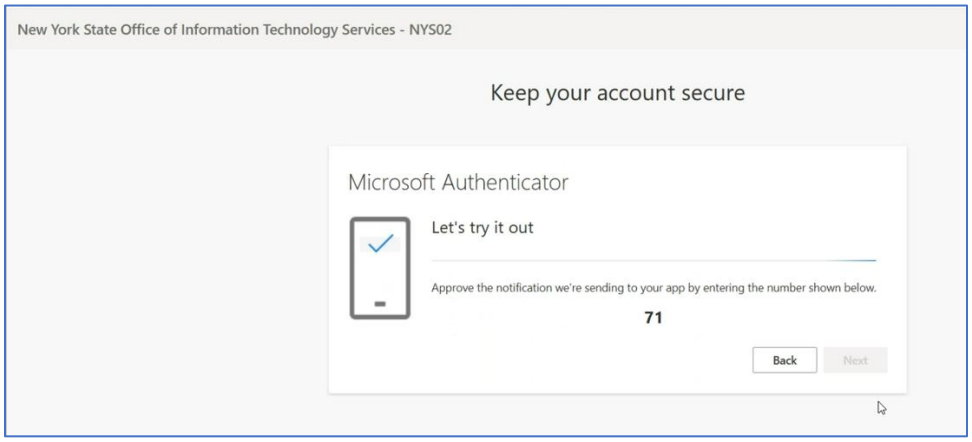
To connect the Authenticator app with your account, use the camera on the phone to scan the QR code.



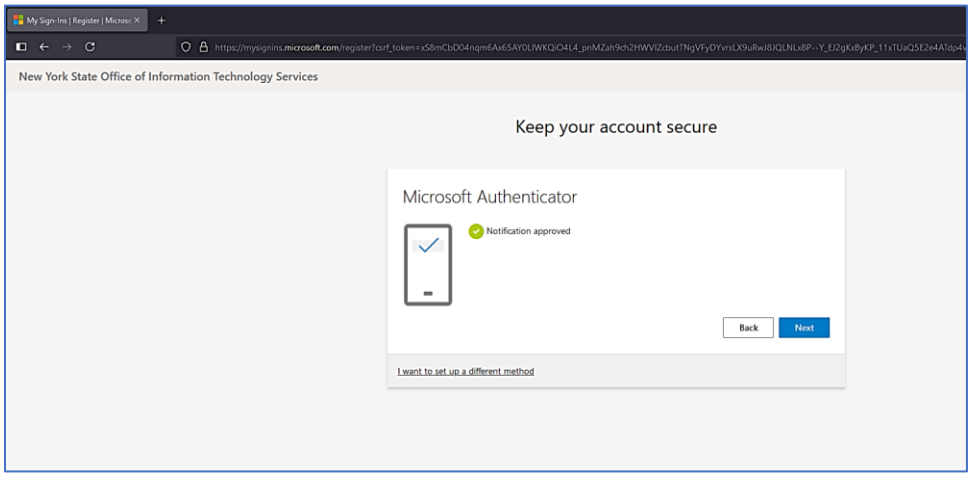
After scanning the QR code on the phone, Click Next



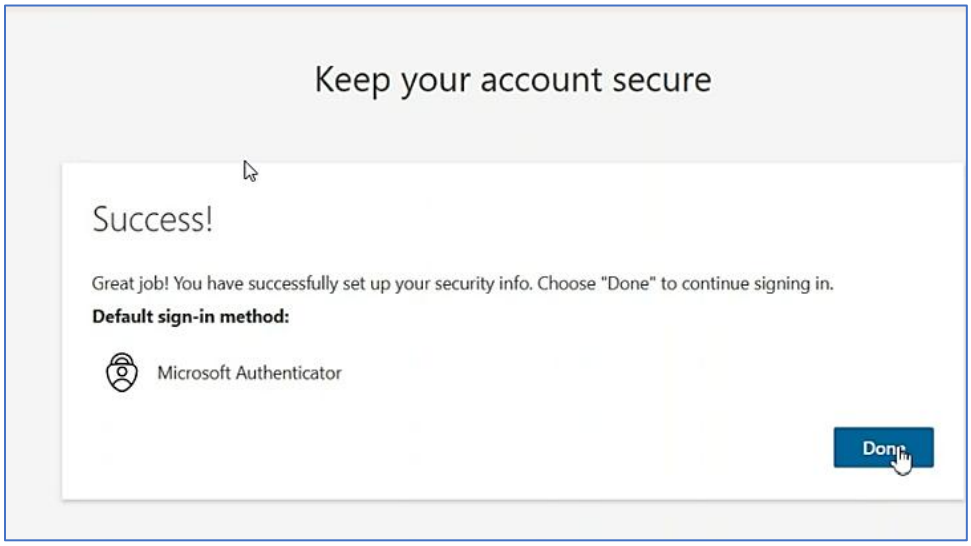
The user will need to approve the notification sent to your app. Enter the number shown on the screen into the Authenticator app.



The authenticator notification is now approved for this phone. Click Next.



The user has now successfully setup multifactor authentication for CHOICES. Click Done.

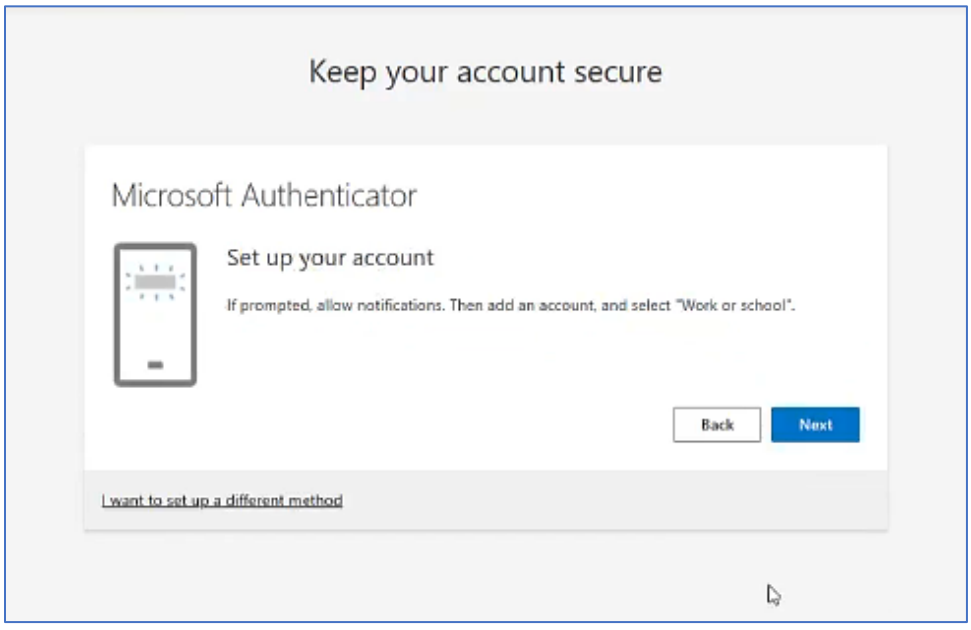


The user will see the Apps dashboard page. This will complete the initial user account set up process. User may close the browser.

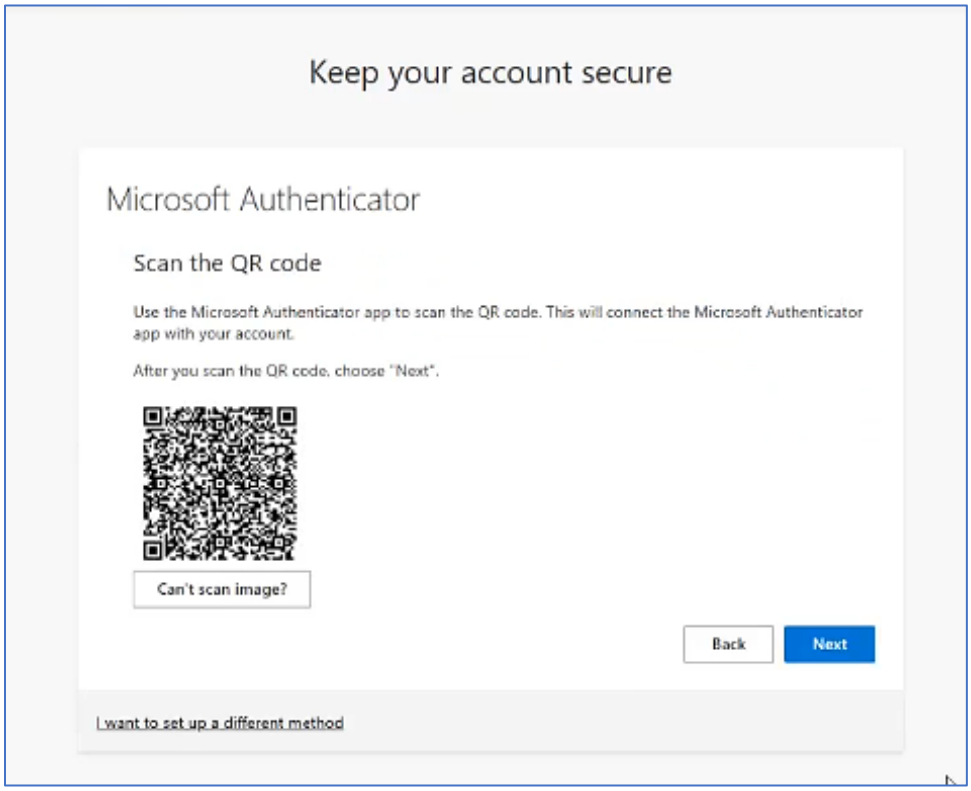
2.1 MFA – MS Authenticator pre-installed

The following instructions are for the user who already has the Authenticator app downloaded on their phone and intends to use that as the MFA for CHOICES.

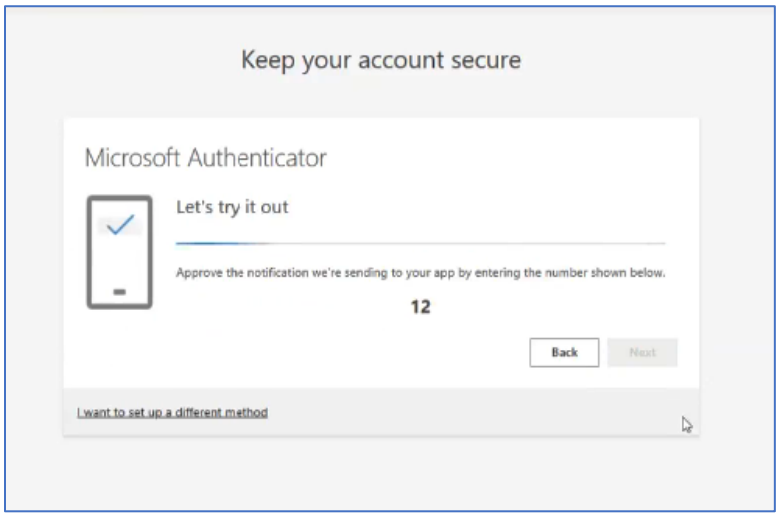
At this screen click Next.



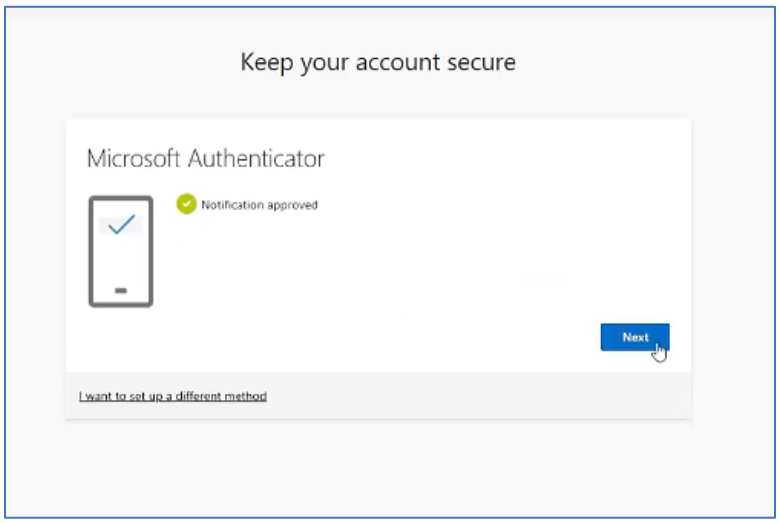
At this screen the user is asked to scan the QR code with their Authenticator app, not the phone camera. Follow the instructions on your phone, then click Next.



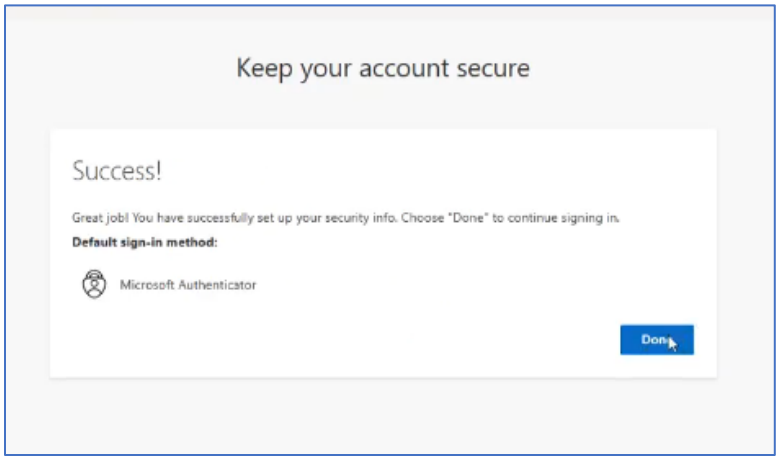
The next step is to verifiy the Authenicator app is working correctly. Enter the number shown on your phone in the Authenticator app.



The user is notifiied the connection to CHOICES has been approved. Click Next.



User is notified the set up of adding CHOICES to your Authenticator app has been successful. Click Done.

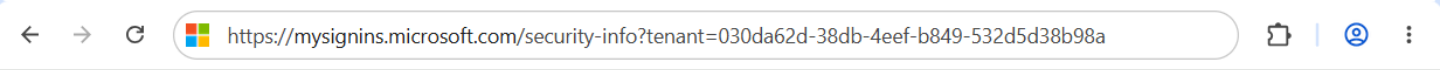


3. Updating MFA Settings

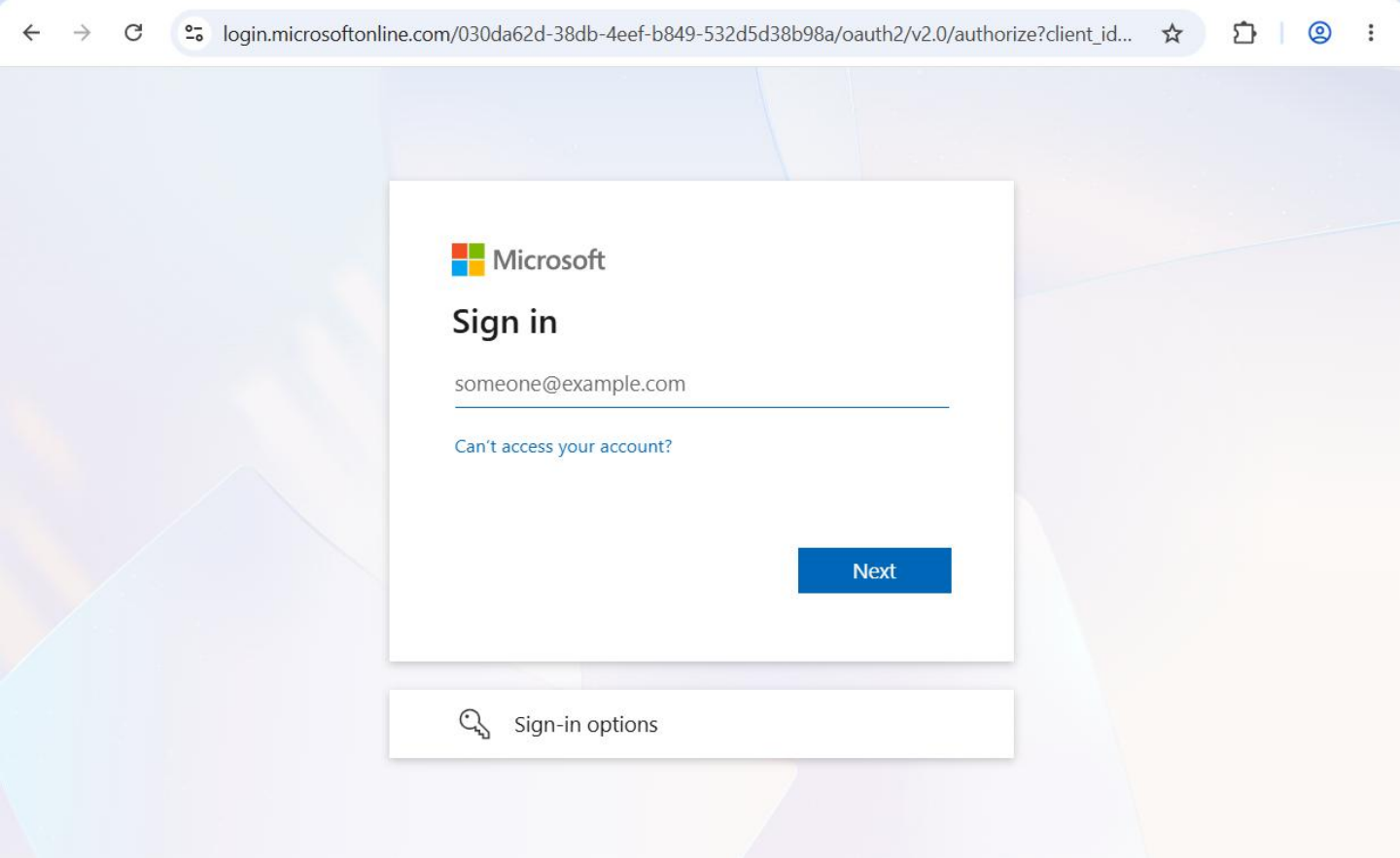
This section applies if you would like to add an additional MFA sign-in method (phone or MS Authenticator) to your account, or if you are trying to set up MFA on a new cell phone and still have access to the old phone.

To change Security Settings, navigate to this URL:

https://mysignins.microsoft.com/security-info?tenant=030da62d-38db-4eef-b849-532d5d38b98a



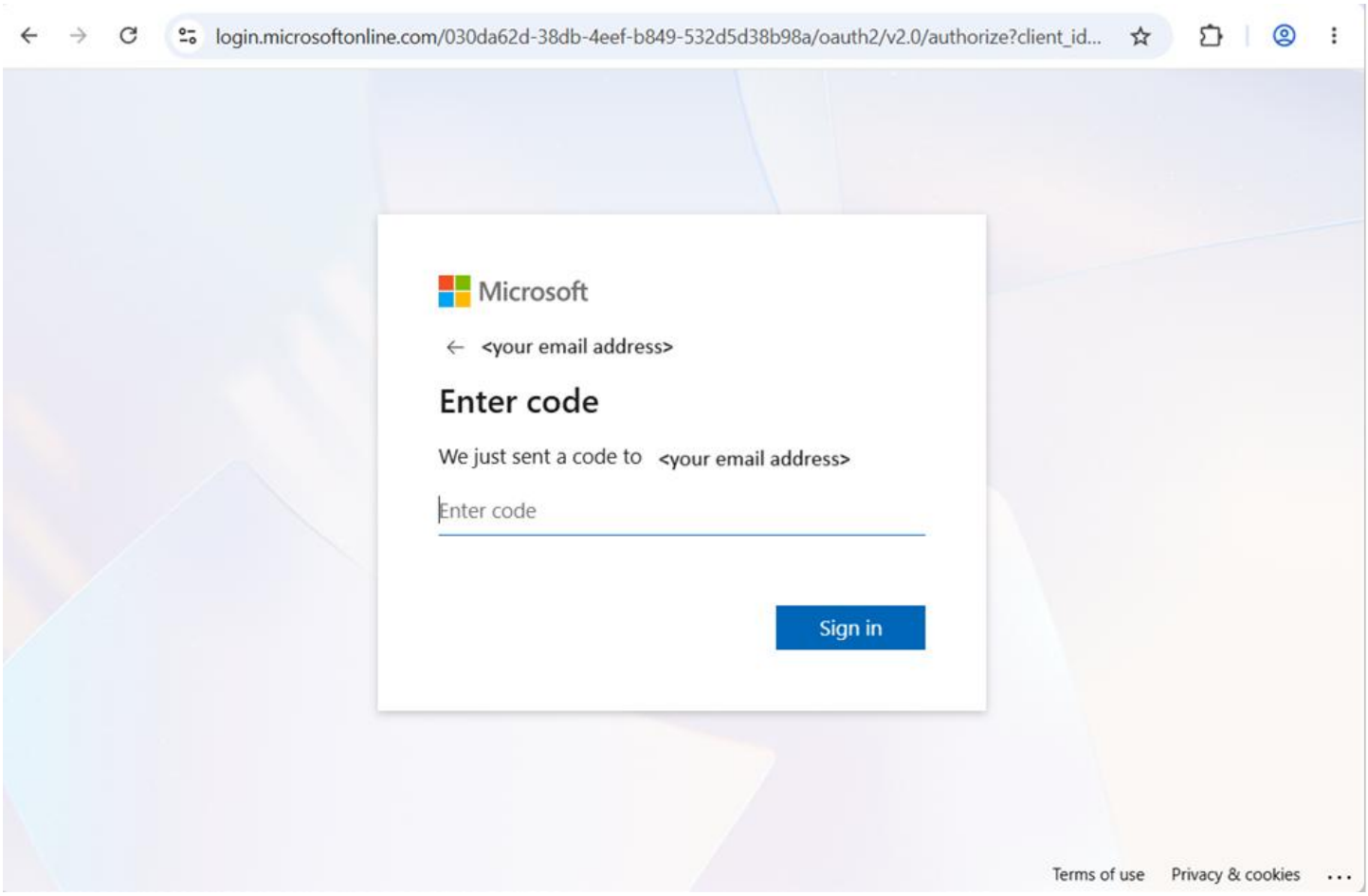
You will be re-directed and asked to sign in. Enter your Agency E-mail address and click Next.



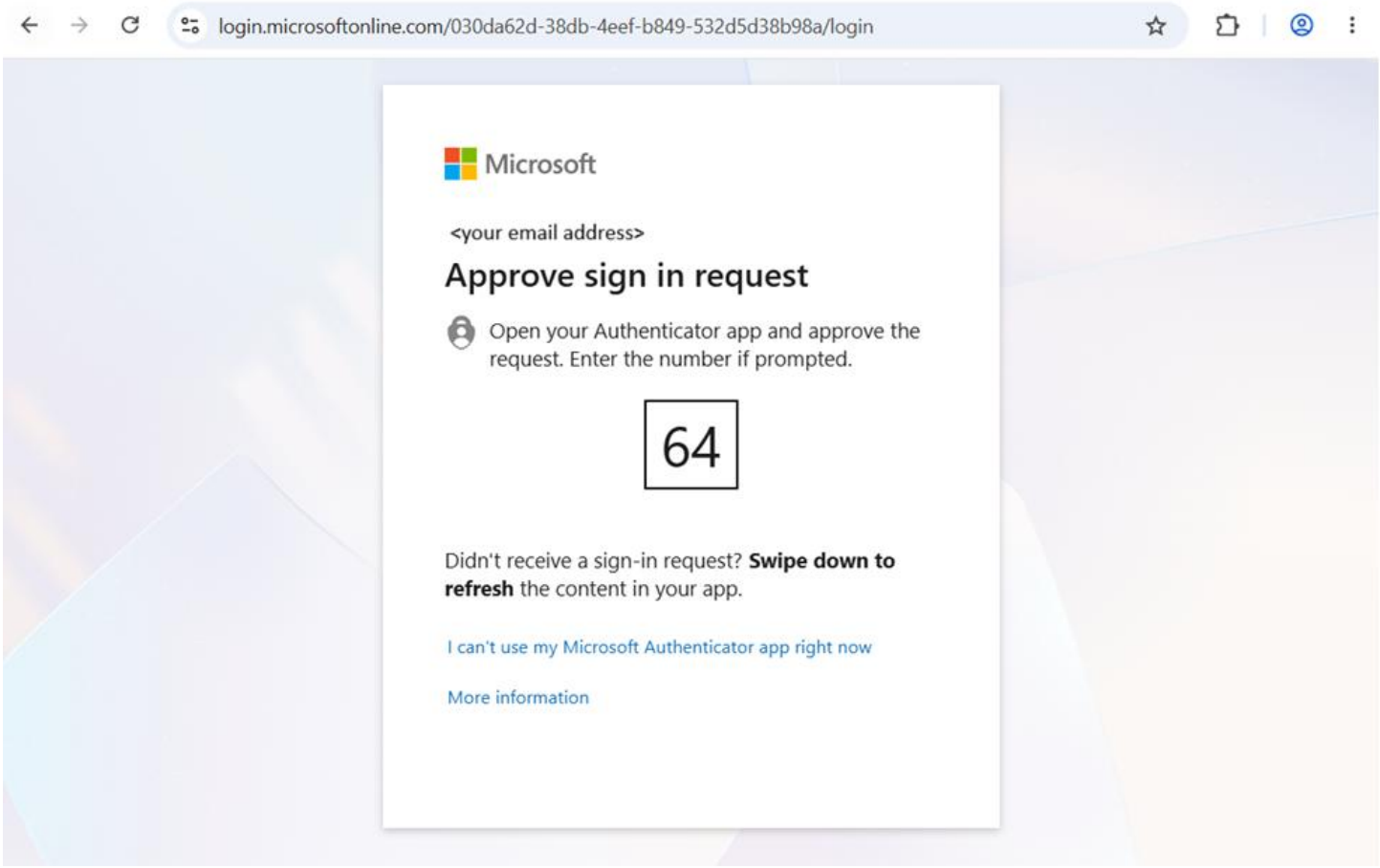
At this point, depending on your organization's settings and sign-in method you will either:

- Be re-directed to your organization's sign-on page to sign-in with your Organization e-mail address and password (continue to the next page of these instructions after doing this)
- Be asked to enter the one-time passcode sent to your e-mail address

If you use a one-time passcode code to sign in, enter that on the next screen and click Sign in

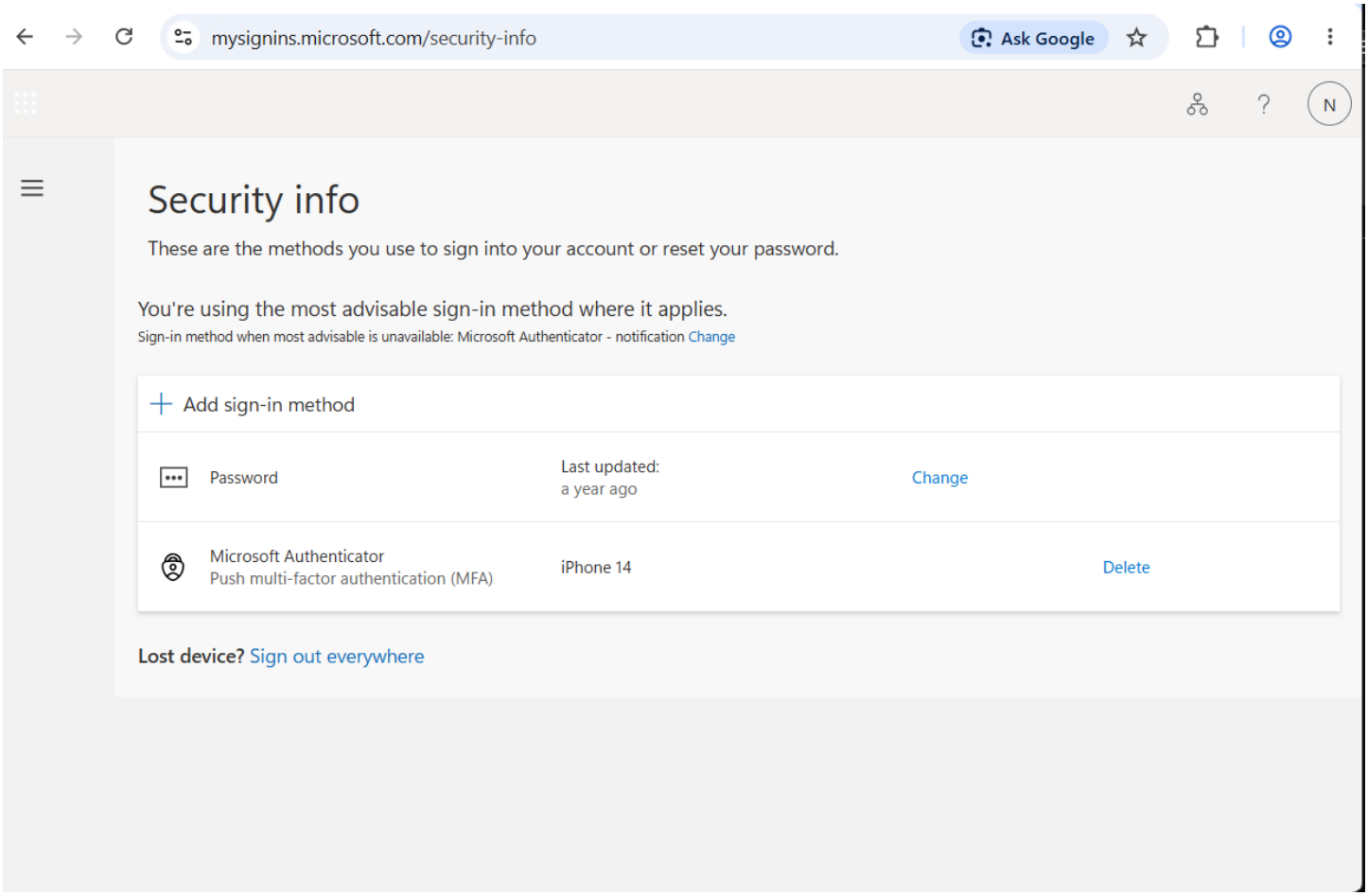


Enter your MFA code into the Authenticator app on your original device to complete sign in

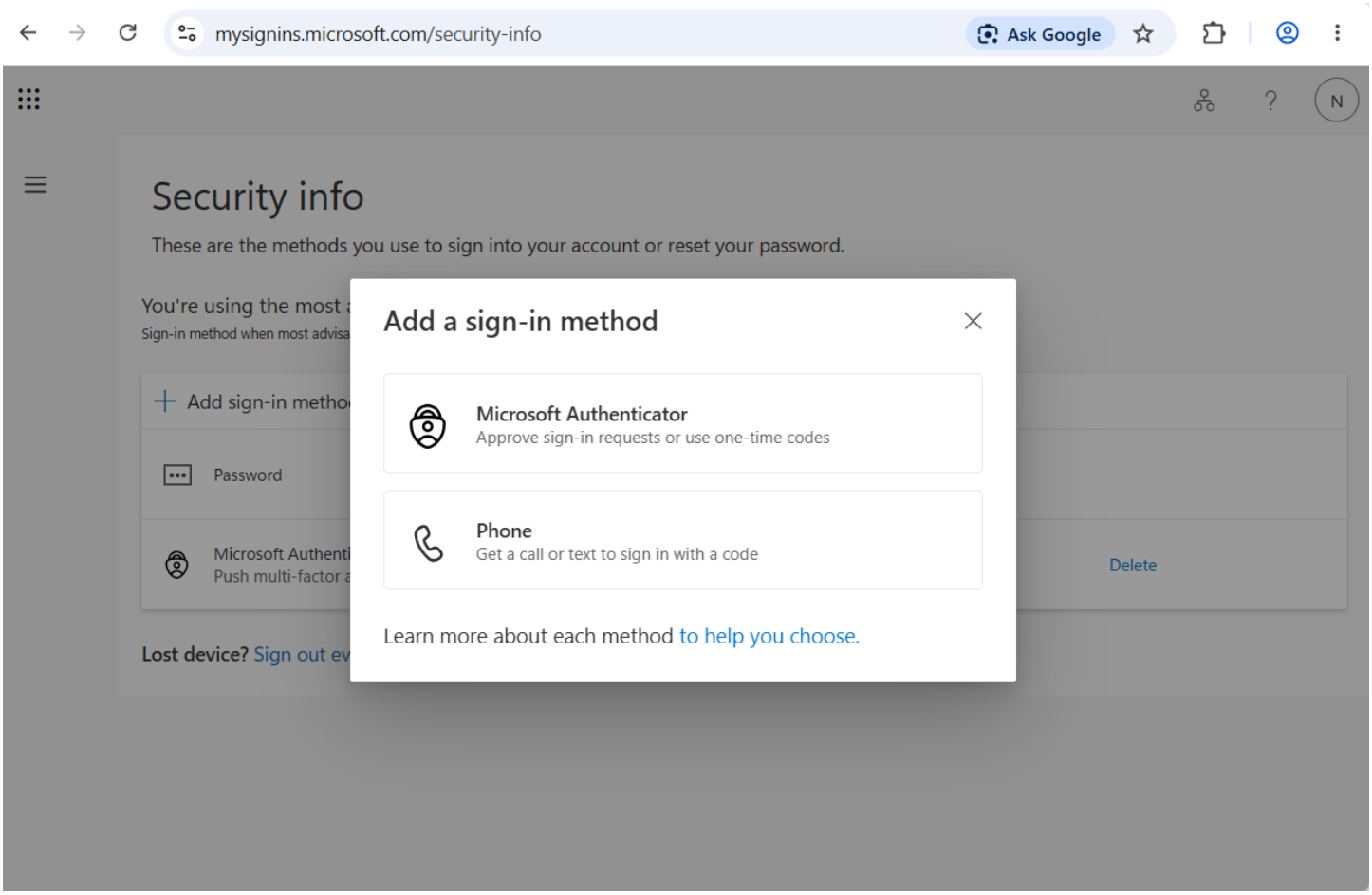


Note: In this example, we're using the MS Authenticator App, but you could also enter a text message code here if that was what you had previously chosen as your form of MFA.

Once signed in, on the Security Info screen, click +Add sign-in method



On the pop-up menu, choose whether you will be using the Microsoft Authenticator or Phone (Note: The phone option works for text messages only, not phone calls).



Once you select a method, follow the additional steps presented on the screen to complete setup.