

VPCC Initial logon and MFA Authentication Setup

The purpose of this document is to walk you through the initial login with your new Virginia Peninsula Microsoft 365 sign in and setting up multi-factor authentication (MFA).

MFA is an extra verification step done through a combination of your username, your password, and a mobile device or phone.

You will need these instructions to access email using the web browser or any remote work. These instructions do not include logging into a domain joined computer on campus if you will not be using Microsoft 365 (formerly Office 365).

This setup will require you to access your cell phone and the website simultaneously during the completion of the process. Best practice is to use a PC/Mac AND your mobile device to setup MFA.

Initial Sign-In at Microsoft 365

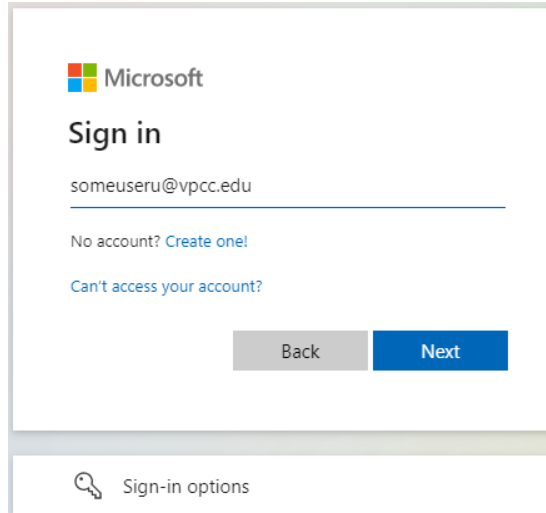
To begin the process, follow these steps:

1. In your preferred browser, go to <https://office.com> and select **Sign in**.



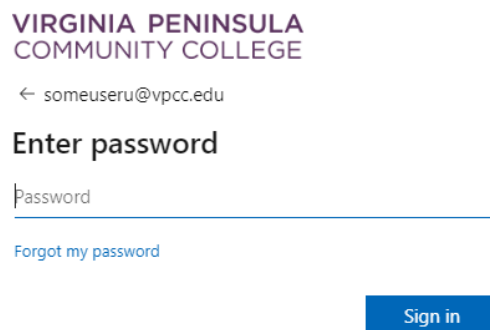
If you do not see the option to **Sign In** here, it means that you are already signed in with another work or school account. You will need to sign out of your other Microsoft 365 account first or use another, separate browser, to sign into your VPCC account.

2. Enter your VPCC email address at the prompt and select **Next**.



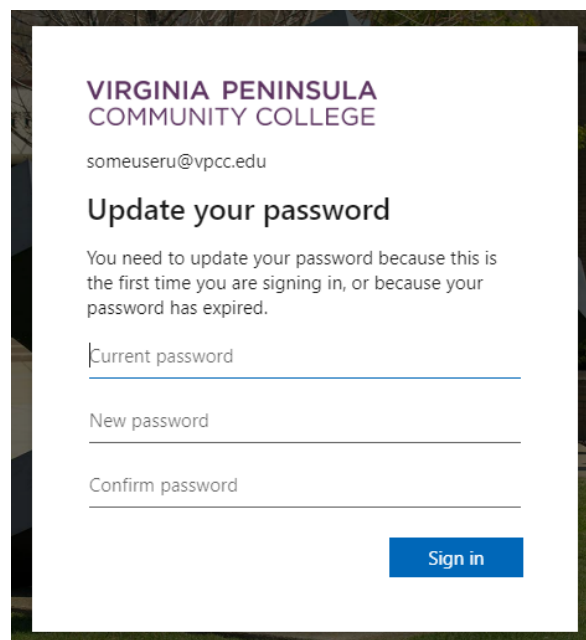
Microsoft
Sign in
someuseru@vpcc.edu
No account? [Create one!](#)
[Can't access your account?](#)
Back Next
Sign-in options

3. Enter your password and select **Sign in**.



VIRGINIA PENINSULA
COMMUNITY COLLEGE
← someuseru@vpcc.edu
Enter password
Password
[Forgot my password](#)
Sign in

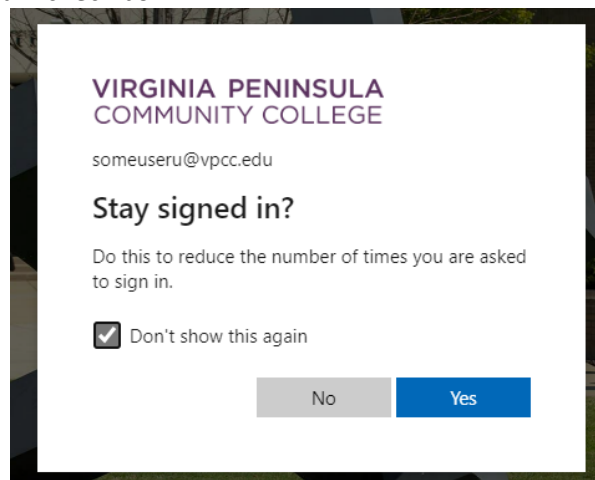
4. If this is your first time signing in, you will need to change the initial password you were given.



VIRGINIA PENINSULA
COMMUNITY COLLEGE
someuseru@vpcc.edu
Update your password
You need to update your password because this is the first time you are signing in, or because your password has expired.
Current password
New password
Confirm password
Sign in

VPCC Account Password Requirements

- Passwords must be reset every 180 days.
 - Password must not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
 - Cannot re-use previous passwords.
 - Be at least thirteen characters in length.
 - Contain characters from three of the following four categories:
 - English uppercase characters (A through Z)
 - English lowercase characters (a through z)
 - Base 10 digits (0 through 9)
 - Non-alphabetic characters (@ # \$ % ^ & * _ ! + = [] { } | \ : ' , . ? / ` ~ " () ; < >)
5. Choose to stay signed in, or not, either choice works. It's a matter of preference. Same with the *Don't show this again* check box.



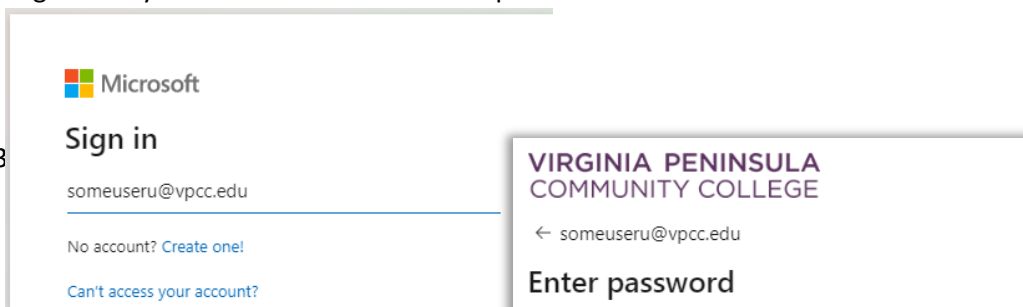
Multifactor Authentication

The first time you complete your sign in you will need to setup a Multifactor Authentication (MFA).

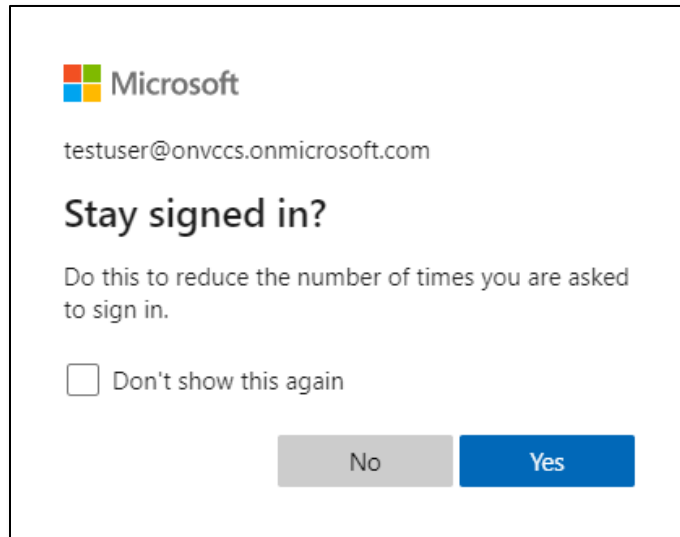
Install and set up the Microsoft Authenticator app

It is highly recommended that you use the Microsoft Authenticator for MFA for VPCC Microsoft 365 access. If not already installed on your device, typically your smartphone, you will download the Microsoft Authenticator app and set it up to receive a push notification for approving or denying an authentication request. This method is fully supported by VPCC IT and Microsoft.

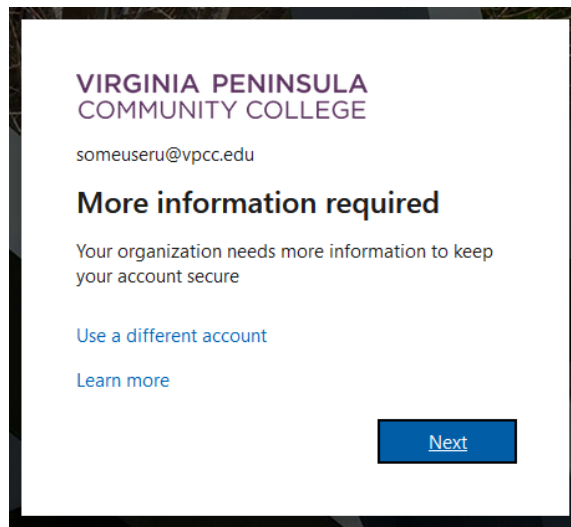
1. Download the Microsoft Authenticator app to your mobile device. You can use this link, https://www.microsoft.com/en-us/security/mobile-authenticator-app?cmp=zgcv4w_ifocsj, to find the app or search for it in Google Play Store or Apple App Store.
2. Open a web browser on a separate device from your phone and go to <https://aka.ms/mfasetup>.
3. Log in with your VPCC email address and password:



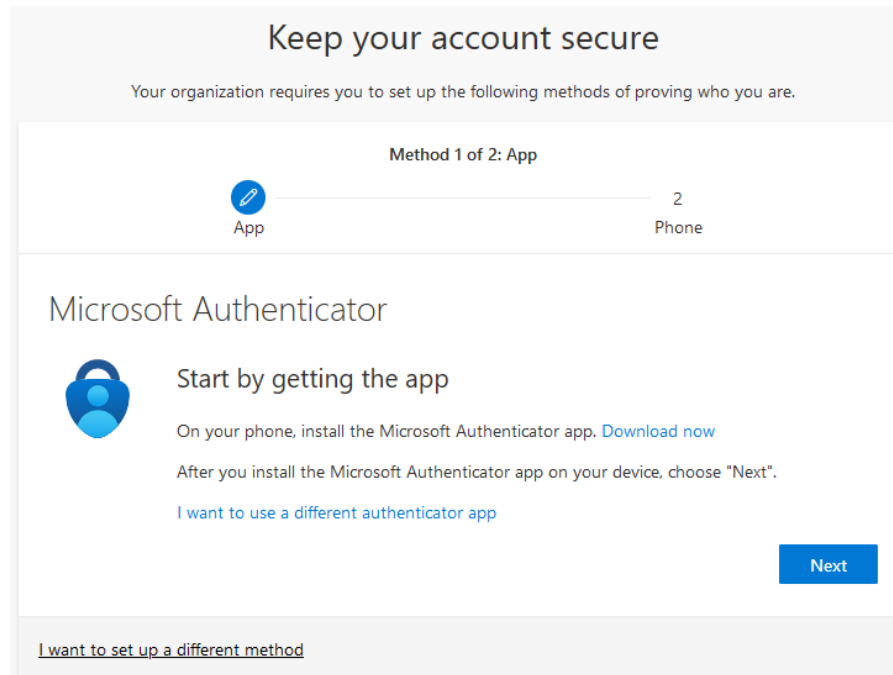
4. You may receive the following. Choose any option here. It's your preference.



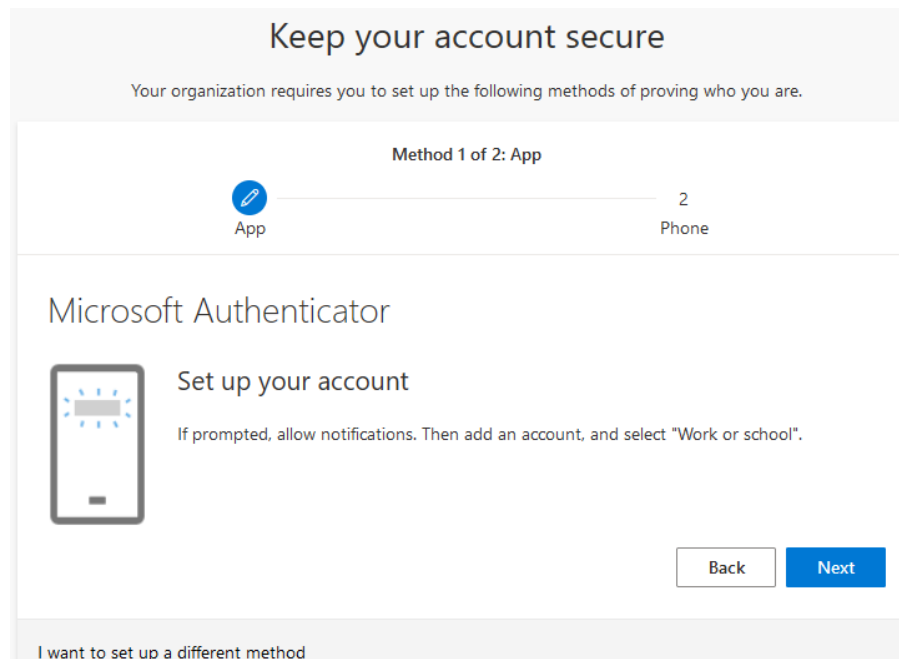
5. Click **Next**.



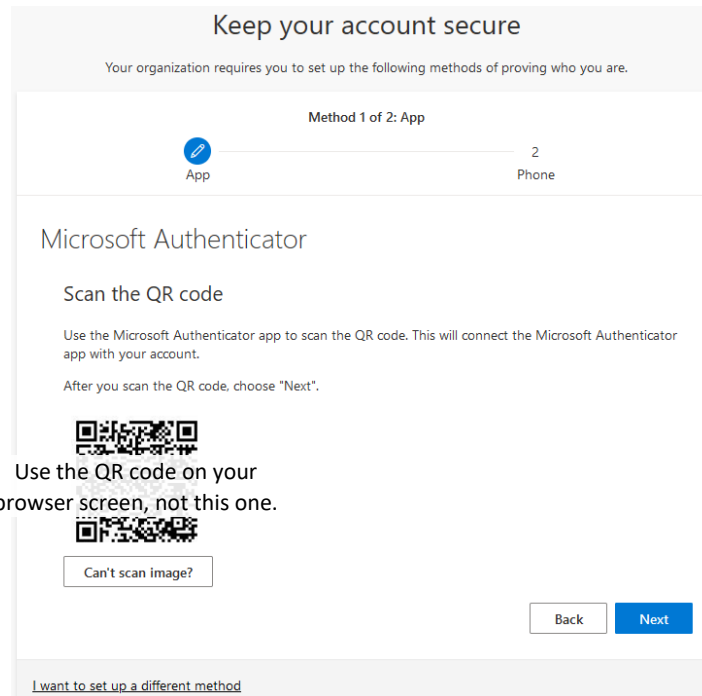
- If you did not install the Microsoft Authenticator app in step 1 above, do it now using the *Download now* link provided. Click **Next**.



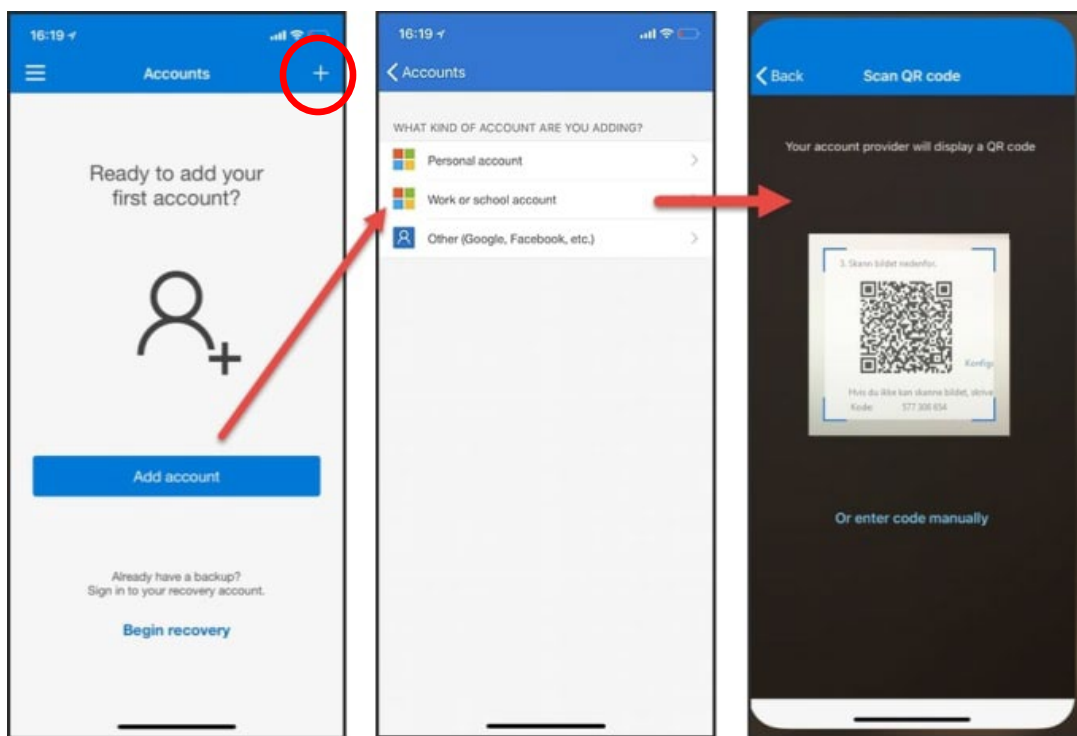
- While still in web browser on your computer, Click **Next**.



8. This will bring up the following screen with a QR code on your computer. **Before clicking on the Next below, open the Microsoft Authenticator app on your mobile device.**



You are looking for the option to add a new account, which will be via the plus sign or by selecting the three vertical dots. If option isn't visible, select skip or cancel to continue to app's home screen.

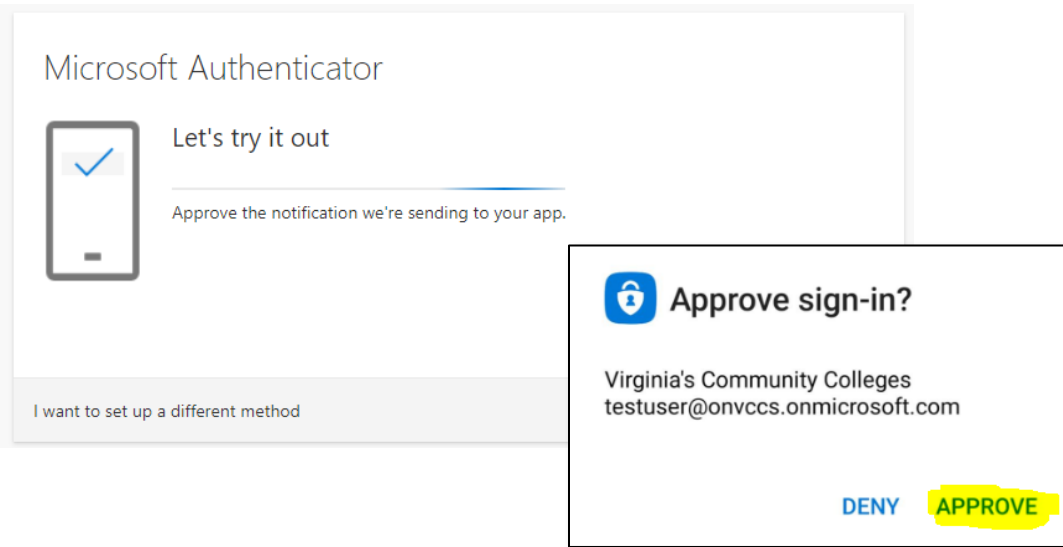


Once found, select **Add Account**. Select **Work or school account** then select **Scan a QR code**.
Note, you want to allow the Camera permission!

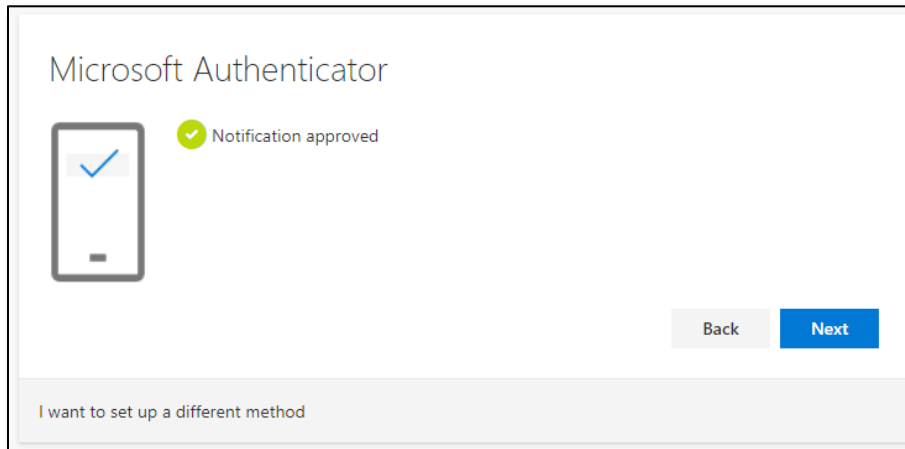
Using your mobile device, scan the QR code displayed in your computer's web browser.

Once complete, click **Next** on the Scan QR code screen above.

9. While the following is present in the web browser, you should have received a notification on your mobile device. Click **Approve** on your mobile device.



10. In the web browser, you'll see the following. Click **Next**:



11. Enter your mobile phone number for a second method of authenticating in case you have problems using Authenticator.

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Method 2 of 2: Phone

App Phone

Phone

You can prove who you are by answering a call on your phone or texting a code to your phone.

What phone number would you like to use?

Text me a code
 Call me

Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).

[I want to set up a different method](#)

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Method 2 of 2: Phone

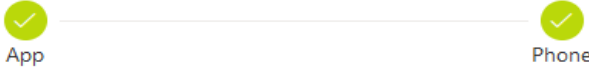
App Phone

Phone

SMS verified. Your phone was registered successfully.

12. You are done! Click the **Done** button.



Method 2 of 2: Done



Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method:

-  Phone
+1 703 252 2222
-  Microsoft Authenticator

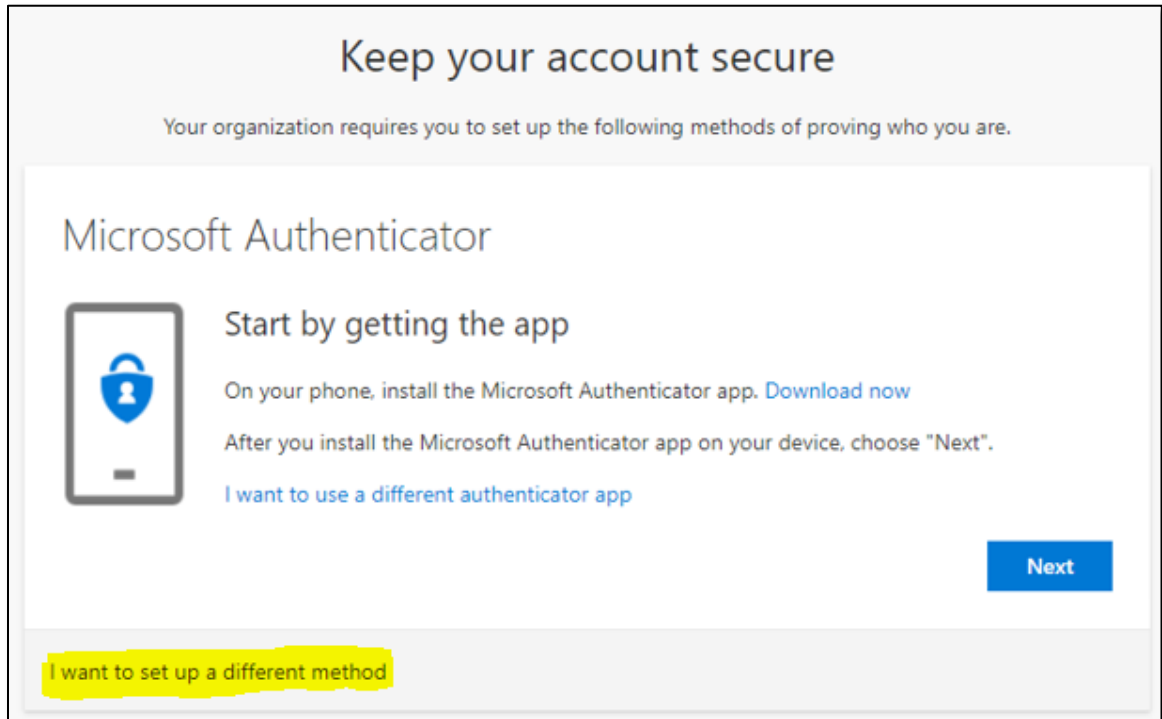
[Done](#)

Set up a different method

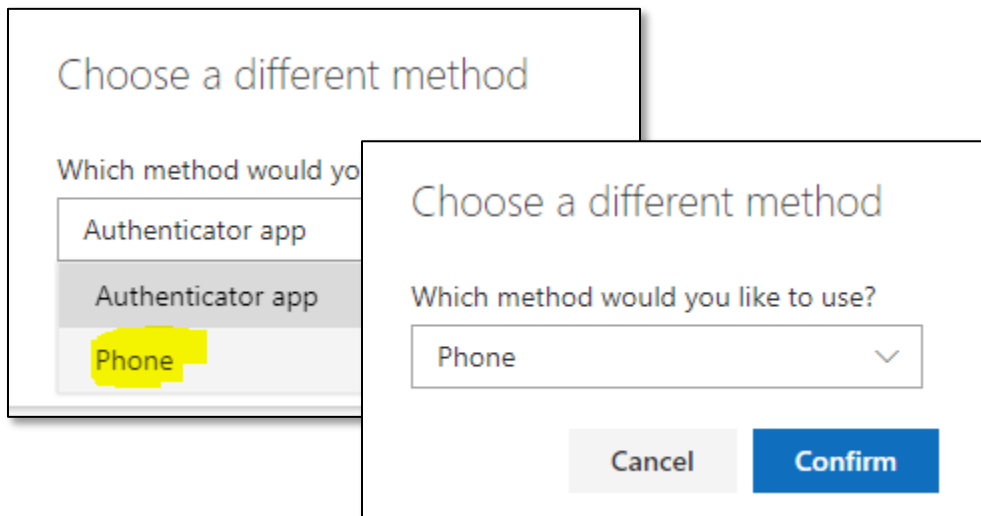
If you set up the Microsoft Authenticator app above, you are done. You do not need the following.

If you are not able to use an authenticator app, you can set up your phone (desk or mobile) to receive a phone call from Microsoft. **This method is NOT recommended.** If you must use this method, your mobile phone is your best choice. If you choose a desk phone, you will not be able to sign in to office.com and use your email unless you are at your desk phone.

1. Click on the **I want to set up a different method**:



2. Choose the **Phone** option, then click **Confirm**:



3. Add your phone number and click **Next**:

Phone

You can prove who you are by answering a call on your phone.
What phone number would you like to use?

United States (+1) Enter phone number

Call me
Message and data rates may apply.

Next

I want to set up a different method

4. You will receive a phone call from **855-330-8653**. Follow the instructions and once complete, click **Next**:

Phone

Call answered. Your phone was registered successfully


Next

5. You are done! Click the **Done** button.

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method: Phone - call 8044238941

 Phone
+1 8044238941

Done