Office of Information Technology

Two-Factor Authentication (2FA) Instructions

This document contains important information and resources you will need to review to help ensure the successful setup of 2FA for your account.

2FA will only be in effect when you are off-campus. You will not be required to use 2FA when connecting on the Webster network (including campus housing in the dorms/apartments), however, the first time you logon to Connections after 2FA is turned on for your account whether on campus or off, you will need to setup your security options and secondary authentication method, or complete 2FA authentication to your phone number or Authenticator App if you already have one set as your default sign-in recovery/authentication option.

Step #1: Log into Your Connections Account

Step #2: Setting Up Security (2FA) For Your Connections Account

- Option #1: Downloading and Configuring Microsoft Authenticator App
- Option #2: Configuring Phone as Primary Authentication Method

Setting Up Additional Security/Recovery/Authentication Methods

Remember Your Device & Using the "Sign in a Different Way" Method

Step #1: Log into Your Connections Account

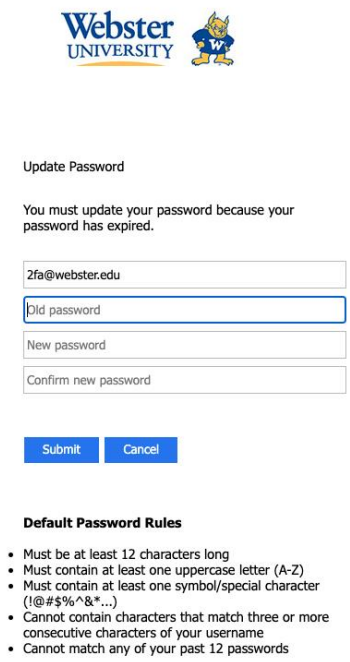
NOTE: *If you will be using the Microsoft Authenticator App as your primary 2FA method and do not already have it configured, please ensure you have access to both a computer and your smart device or mobile phone before completing these steps as both will be required to complete the 2FA configuration.*

1. Open any browser of your choice using a computer and go to https://connections.webster.edu.
   - Enter your @webster.edu email address. You will be redirected to our Webster University sign-in page. (see below)
   - New Employees/Students – You would have received a temporary password for your newly created account to log in.
   - Employees/Students with Existing Accounts – Please use your existing password to log in.

New Employees/Students

This section is for **new** employees/students who are setting up their account for the first time. If you are an existing employee/student who already has their account set up, please skip to the next section.

2. Enter your temporary password and hit **Sign In**. Your temporary password typically follows the format of first letter of first name capitalized, first letter of last name lowercase, 7 digit Webster ID number, hashtag (#) sign (i.e. Js1234567# where 1234567 is your own ID number). You will receive a message that your password has expired and needs to be updated (see below). Enter your temporary password again in the **Old password** box and then proceed to create a new password for your account in the third and fourth boxes. Your password must meet the criteria at the bottom of the page. Click **Submit** when done.



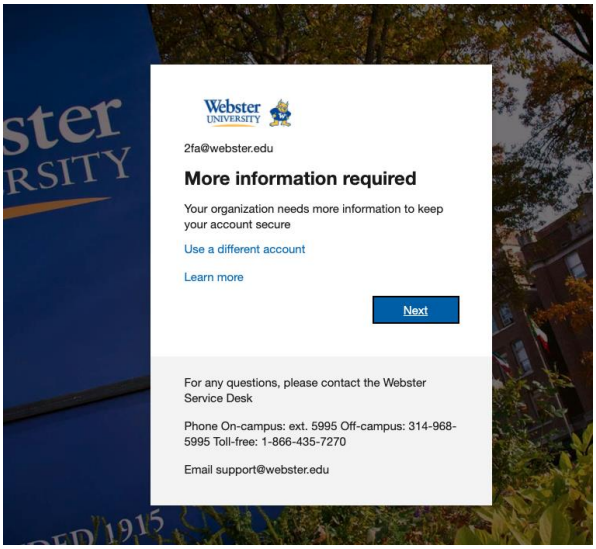
3. After you create your new password, go back to https://connections.webster.edu and sign in with your updated login information. Then proceed to the next section for further instructions regarding your 2FA setup.

Step #2: Setting Up Security (2FA) For Your Connections Account

The steps to follow next will depend on whether you have a phone number or the Microsoft Authenticator App already configured as the primary sign-in recovery/authentication option. If you already have a phone number/Authenticator App registered, you will instead receive a prompt to enter the code sent to your device

in order to login. If this applies to you, you can skip to the *Setting Up Additional Security/Recovery/Authentication Methods* section. For new accounts, or existing accounts that do not have the required authentication methods already set up, please follow the steps below.

4. On the More Information Required screen, click **Next**.



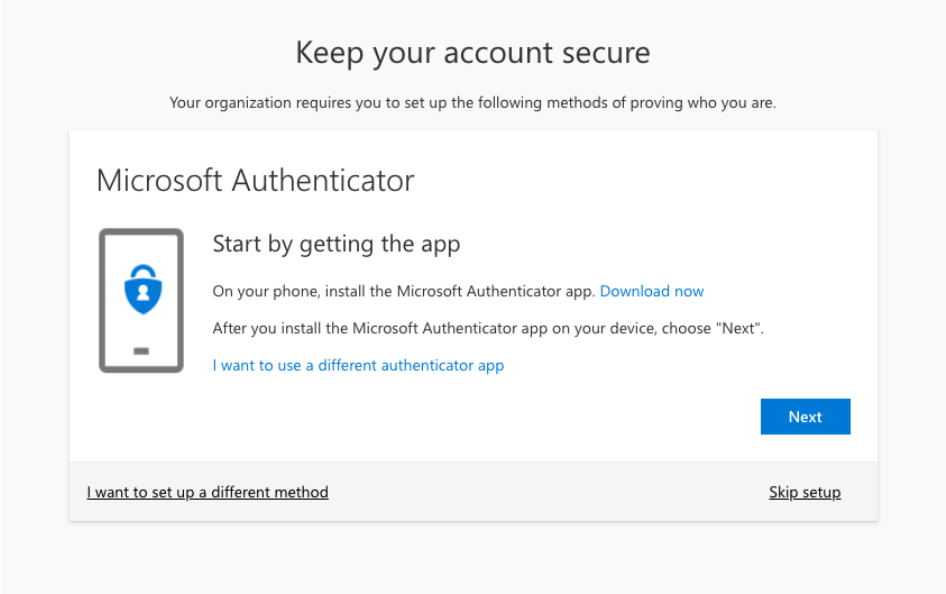
5. You will be taken to the **Keep your account secure** window. Next steps will depend if you choose Microsoft Authenticator or a personal phone number to be your primary 2FA method. We recommend choosing both options if possible. You will find a section later in this document on how to add additional methods to your account.

Option #1: Downloading and Configuring Microsoft Authenticator App

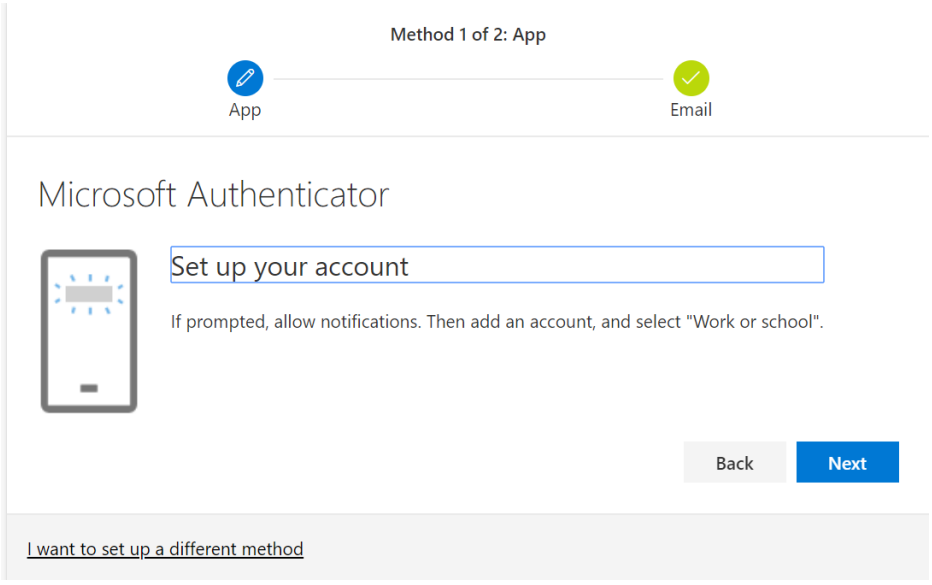
This section will cover how to download and configure the Microsoft Authenticator App. Please remember, this requires having access to both a computer and your smartphone/mobile device. The Authenticator App can only be downloaded to a mobile device. If you do not have the ability to download the Authenticator App right now, please skip to the next section on using the Phone method instead (*Configuring Phone as Primary Authentication Method*). However, if at all possible, we recommend going back later to add the Authenticator App as a secondary recovery option for your account. The 1st method we need to set up for 2FA is “Microsoft Authenticator”.

6. Download the Authenticator App before clicking the Next button on the **Keep your account secure** screen.
   a. Grab your mobile device and download the app from the iOS Apple Store or Android Play Store. You can search for the name "Microsoft Authenticator".
   b. You should now have your computer and mobile phone side-by-side to finish the setup. Proceed to step 7.

7. After downloading the Authenticator App, click on **Next** from the **Keep your account secure** screen as shown in the proceeding image.

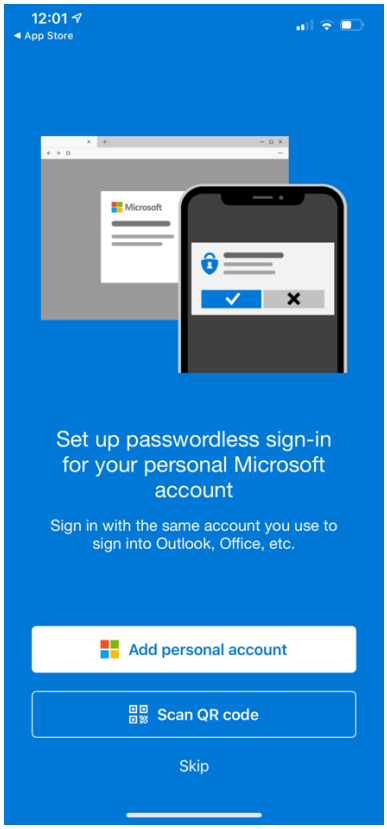


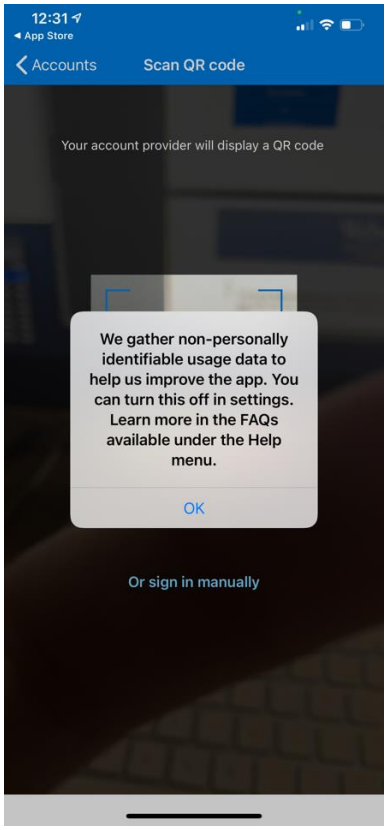
8. On your computer screen, click **Next** again as shown below and have your Authenticator App open. We will be using the Scan QR Code option which will add your account automatically to Authenticator.



9. Using your phone, open the newly downloaded Authenticator app and select **Scan QR Code**. If you do not see the Scan QR Code option when you open Authenticator on your mobile device, click on Add Account in Authenticator and then choose **Work or School**. *You may be asked to allow the app*

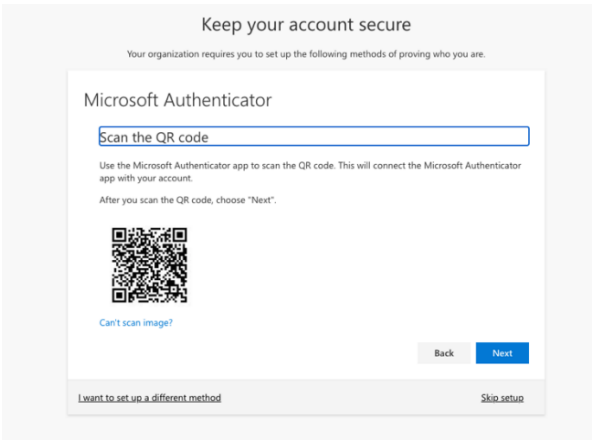
to access your camera. This is necessary to scan the QR code on your computer. See images below. Proceed to next step.

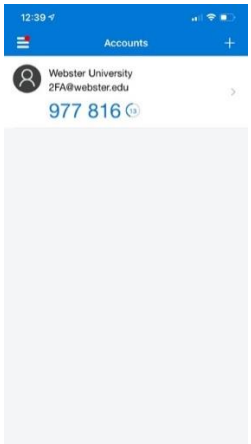




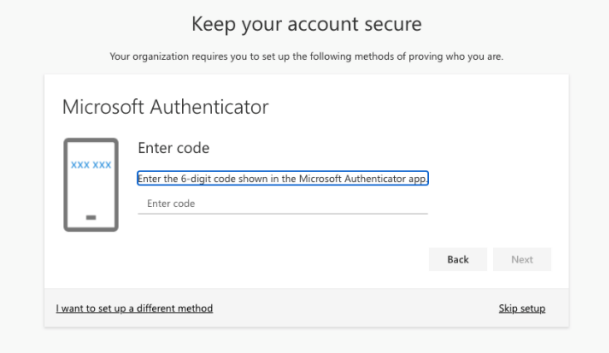
10. On your computer after clicking **Next** above, you will see the image similar to below with a QR code (see image on left).

11. Using your mobile device, align your phone camera with your computer screen and scan the QR Code. It will automatically pull up your account (see image on right) and you should receive a confirmation on your mobile device that the account was added successfully.

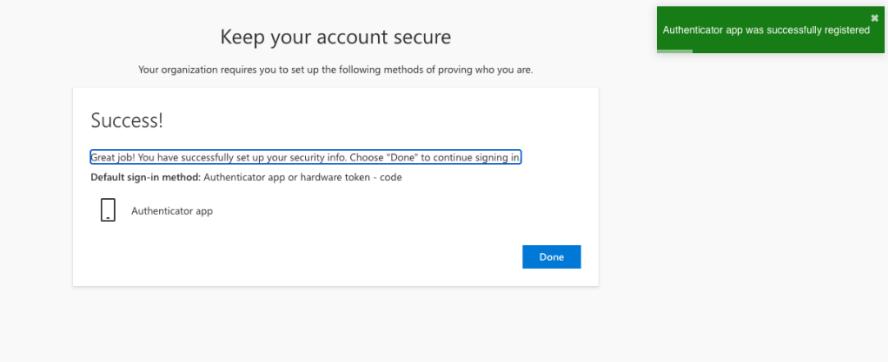




12. On your computer, select **Next**. Here you will type in the 6 digit code that is displayed on your mobile device and click **Next** again. The code updates every 30 seconds. See image below for reference.



13. You will receive a successful confirmation message. Click on **Done** if prompted and proceed to sign in to Connections at https://connections.webster.edu.



IMPORTANT NOTE: You may not receive a 6-digit code to type in via the Authenticator App and may instead simply receive a popup prompt asking you to click on Approve or Deny for the sign-in request. Instead of the screen above to type in a code, you will receive a Notification Approved message after choosing Approve when prompted on your device.

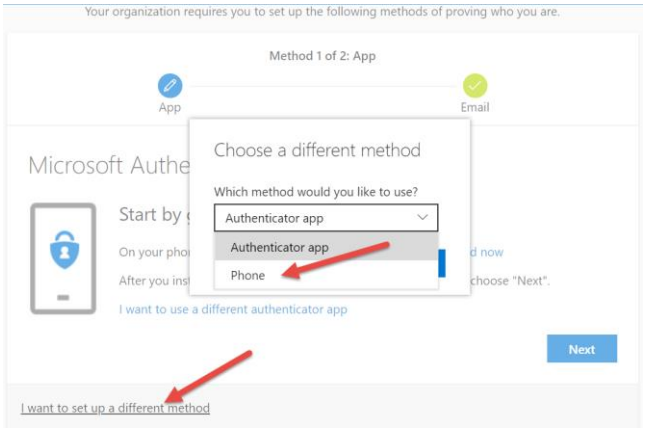
Option #2: Configuring Phone as Primary Authentication Method

After configuring the Authenticator App, you will be asked to choose an additional method to configure. The screen will default to Phone. We highly recommend proceeding with setting up a phone number to use an additional authentication method if you ever run into issues with the Authenticator App so that you have a backup method to sign in.

You should also use the instructions in this section if you do not have the ability to utilize the Authenticator App for a 2FA method and must use Phone as your primary 2FA method

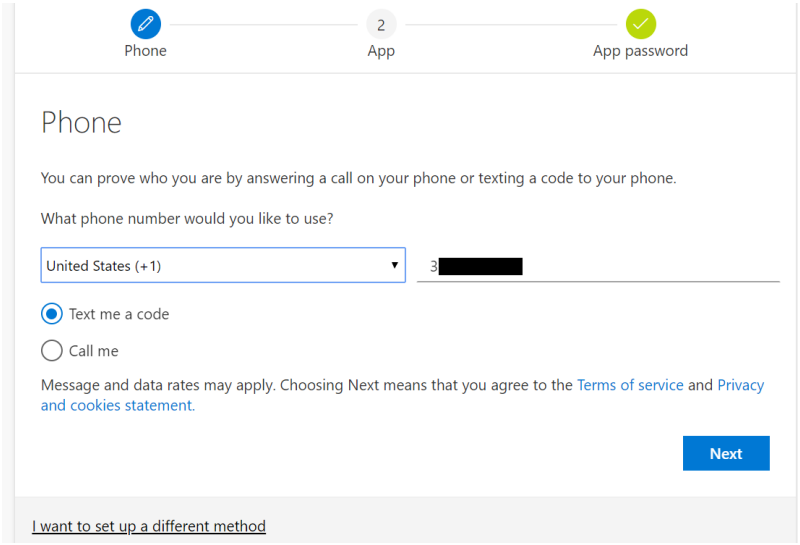
14. If you do not already see the options to enter your phone information, on the **Keep your account secure** window click the **I want to set up a different method** link at the lower right. From the drop-down menu, choose **Phone** and then click **Next**.

    NOTE: If you see an option to use Email in the drop-down menu, this only applies for self-service password resets. Email cannot be used as a 2FA method to log in to your account.

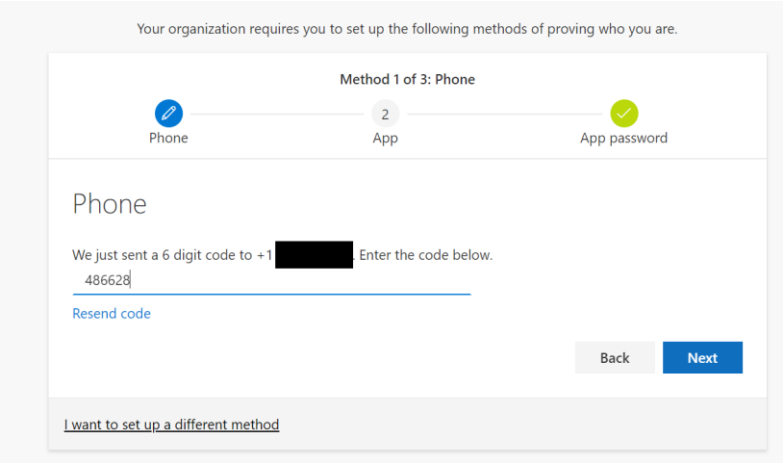


15. On the next screen, choose your Country Code and type in your phone number. Then choose your preference between receiving a code via text or receiving a phone call. Click **Next**.

    NOTE: Be mindful if choosing to call an office telephone number. You would need to have access to that phone off the campus network in order to sign in. It is best to use a personal phone number, and if needed, you can add an additional phone number for backup purposes.



16. You will receive either a text or phone call to the number you provided to verify. If you chose the text option, you will need to type in the 6-digit code you received and click on **Next**.



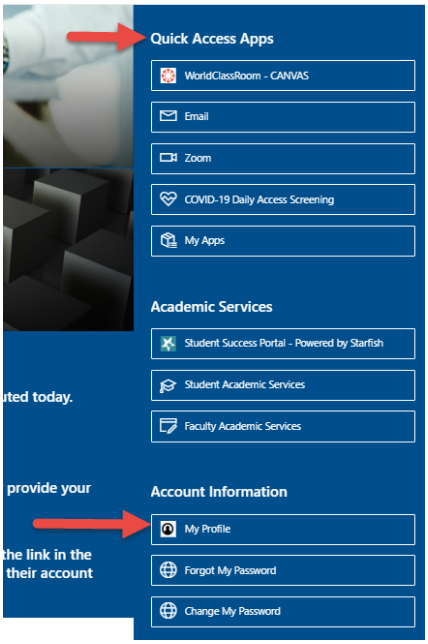
17. You will receive a successful confirmation. Click on **Done** if prompted and then proceed to sign in to Connections at https://connections.webster.edu.

Setting Up Additional Security/Recovery/Authentication Methods

We strongly encourage you to set up multiple to your account for verification. This will be helpful for backup purposes if you do not have access to your default/primary method.

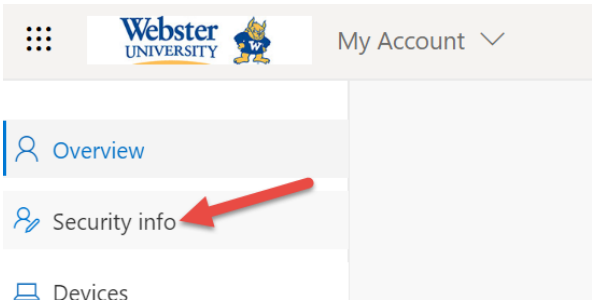
1. Log in to Connections at https://connections.webster.edu.

2. Locate the **Quick Access Apps** section and then scroll down to the **Account Information** section. Click on the **My Profile** link.

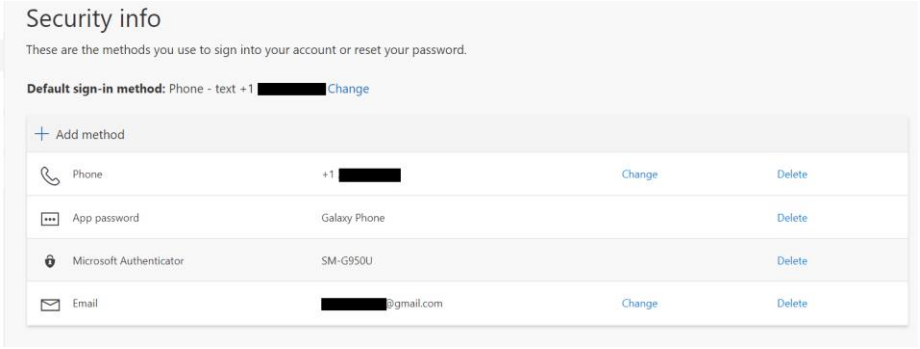


NOTE: You may be asked to verify your security option before accessing this web page

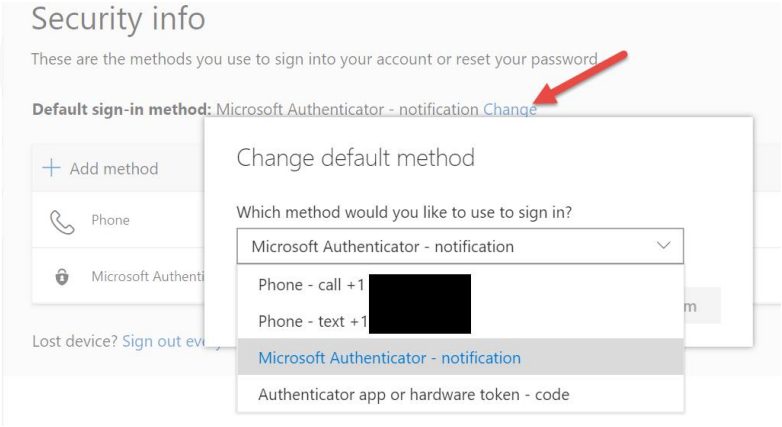
3. Click on **Security Info** from the menu on the left.



4. On this page, you will see the options you configured in the setup process. You will now be able to change your default sign-in method, edit/delete any existing methods and/or add new methods to your account:



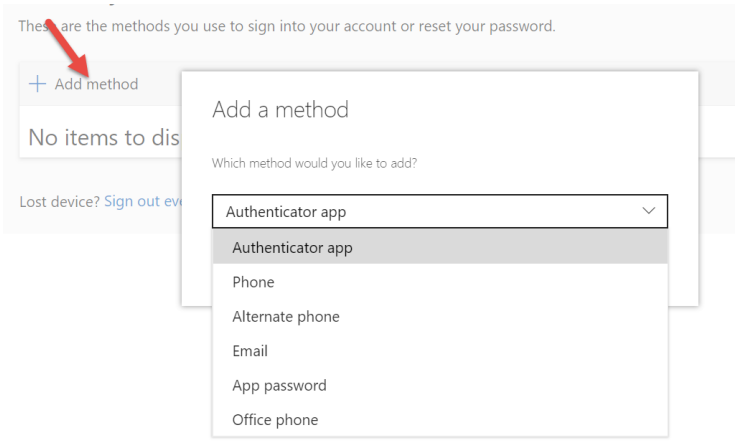
5. To change your default sign-in method, click on the **Change** link next to **Default sign-in method**. You will only be able to choose to call or text a phone number or use the Microsoft Authenticator options.



- Your phone number must have already been added in order to appear in the drop-down. If you do not see a phone number or need to add a new phone number, skip to the next step on adding a new method.
- If using Microsoft Authenticator as your primary method, it will default to **Microsoft Authenticator – notification.** This means that you just receive an Approve or Deny prompt on your mobile device when signing in with 2FA. If you change this to **Authenticator app or**

hardware token – code, this means that instead of only clicking Approve or Deny during the log in process, your Microsoft App will instead display a 6-digit code after you open the app that you will need to type in to the screen on your computer or device you are logging in to your account from.

6. To add an additional method to your account, click on the **+ Add Method** link. You will see some or all of the following options to choose from (depending on what is already set up on your account):



- **Authenticator app** – If you haven't already set up the Authenticator App for your account, we recommend adding this option. Please refer to the Downloading and Configuring Microsoft Authenticator App section on page 3 of this document for further instructions. Please remember you will need both a computer and a smartphone/mobile device to add this option.
- **Phone** – This means a primary phone number to use as your default recovery option. If you already configured this previously, this option will now show up in your list. With your default phone number, you can choose to either text or call you.
- **Alternate Phone** – Use this to add one or more alternate personal phone numbers to your account. If you have already chosen to text another phone number you will only see the "Call me" option available when adding additional numbers.
- **Email** – An alternate email address may be used for the sole purpose of self-service password reset. Microsoft considered alternate email a less secure method and therefore cannot be used for 2FA sign-in purposes.
- **App password** – If you use a service to connect to your Webster account that does not natively support two-factor authentication prompts, you will need to set up individual app passwords for those devices/access methods. Please view the additional resources and FAQs on App passwords and when to use them.
- **Office phone** – You will only have the option to choose "call me" for an office phone. We do not recommend using Office phone as a default sign-in method as this will be dependent on you being able to access your office phone off campus in order to sign in.

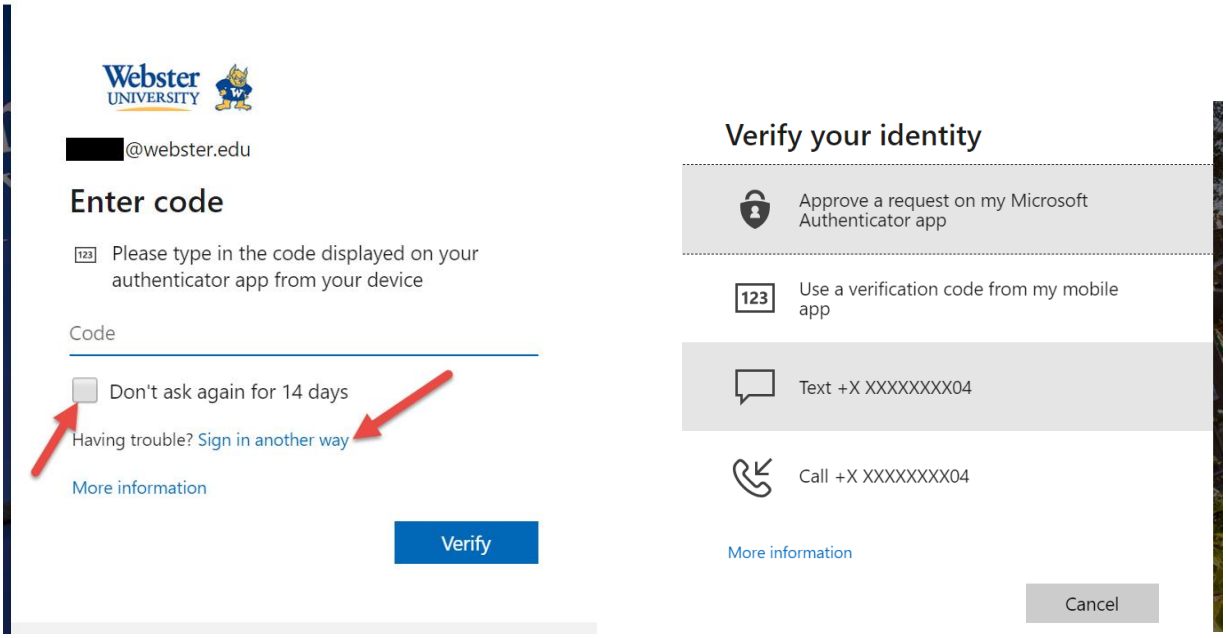
7. Add as many additional methods as you would like and follow the on-screen instructions. Refer back to step #5 for instructions on changing your default sign-in method to a new phone number or the Authenticator App after you add them.

Office of Information Technology

Remembering Your Device & Using the "Sign in a Different Way" Method

When 2FA is enabled on your account, you will be prompted to authenticate via your default sign-in method. The benefit of registering multiple security options is you will have a backup option to sign in to your account if you are having any issues with your primary method.

For example, if you are using the Authenticator App as your primary 2FA method and are having difficulties receiving the code to your device or approving the sign-in, you can click the **Sign in another way** link on the login window as shown below and you will be presented with a list of additional options based on the methods you set up via your security options. You will only be able to choose the Authenticator App or phone numbers.



You also have the option to remember your device for 14 days where you should not be prompted to use 2FA on that device for the next 14 days. You will have to reauthenticate via 2FA when the 14 days are up for that device. To utilize this option check the **Don't ask again for 14 days** box before clicking **Verify** as shown above.

NOTE: This is by device only. If you use multiple devices to access your account, the 14 day countdown will be specific to that device only.