Activating your Penn Highlands Account

You must activate your account to gain access to myPEAK, college email, and on-campus network resources.

If you need assistance during any step of this process, please contact the Information Technology Help Desk at 814-262-6470 or helpdesk@pennhighlands.edu.

Note: Activating your account is a two-step process:

Step 1 - Change Password - You will first need to change your password.

- Log in to Office 365 by entering your college email address which is your myPEAK user name followed by *@pennhighlands.edu and* your temporary password.
- After you log in to Office 365, you will be prompted to change your password. Follow the on-screen directions to change your password.

Step 2 - Create/Edit Profile - Once you change your password, you will be prompted with a screen that states **More information required**. You will need to set up a security profile by enrolling at least one mobile device such as a phone, tablet, and/or another hardware device.

To enroll you can you utilize any or all the following methods:

- Microsoft Authenticator App on your mobile device (**preferred method**)
- Text message with code to your personal device
- Email message with code to your personal Email Address
- Or phone call at your desk/mobile phone

The **Microsoft Authenticator** app is the preferred method and helps you sign-in to your accounts using two-factor verification. Two-factor verification helps you access your accounts more securely, since passwords can be forgotten, stolen, or compromised, two-factor verification is an additional security step that helps protect your account by making it harder for other people to break in.

To download the Microsoft Authenticator App, visit the app store on your device:

https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en_US

https://apps.apple.com/us/app/microsoft-authenticator/id983156458

Note: You'll only see this prompt if you haven't set up the security info required by your organization. If you've previously set up your security info, but if you want to make changes, you can follow the steps in this how-to article Add or update your security info overview or visit https://aka.ms/mysecurityinfo.

If what you're seeing on your screen doesn't match the steps in this document, it means that your account is not set up for Activation. Please contact the Information Technology Help Desk at 814-262-6470 or helpdesk@pennhighlands.edu.

You will need the following information to activate your Penn Highlands Account:

1. **User Name** - This was emailed to your personal email account that you specified on your College Application. You would have received this after you were accepted to Pennsylvania Highlands.

2. **Email Address** - Your Penn Highlands email address is your myPEAK user name followed by *@pennhighlands.edu*, for example, a111a1@pennhighlands.edu

3. **Password** - Your temporary password is made up of the first 3 letters of your **county** name followed by your **zip code**.

   For example, if you lived in Cambria County and your zip code was 15904 your initial password would be: **Cam15904** (*Please make sure to capitalize the first letter as your password is case sensitive*).

   Note: If you are an out of state student your initial password will be made up of the first 3 letters of your state name and your zip code (e.g. Mar21517)
   For example, if you lived in in the state of Maryland and your zip code was 21517, your initial password would be: **Mar21517**

Follow the remaining instructions in this document to Activate your account and Set up your security profile.

Sign-in to your Penn Highlands Office 365 account

After you sign-in to your Penn Highlands Office 365 account at https://www.office.com.

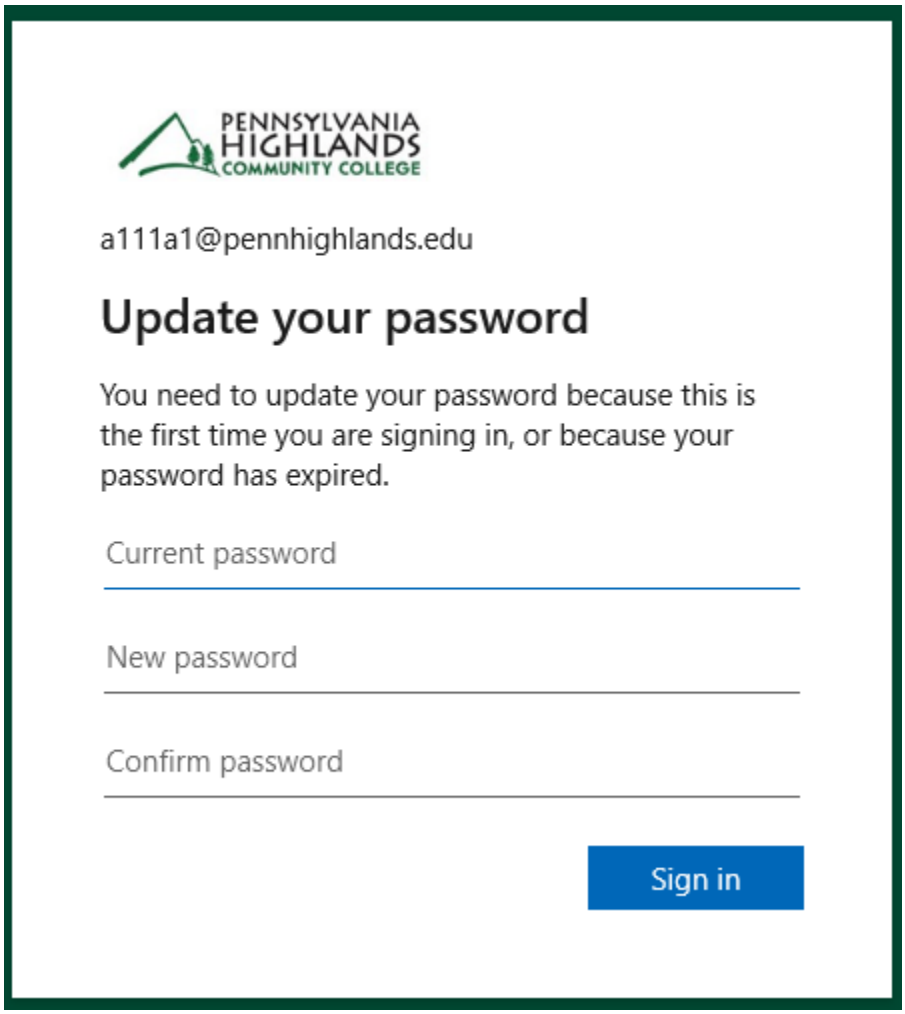
You will then need to sign -in with your email address and temporary password.

PENNSYLVANIA
HIGHLANDS
COMMUNITY COLLEGE
← a111a1@pennhighlands.edu
Enter password
Password
Forgot my password
Sign in

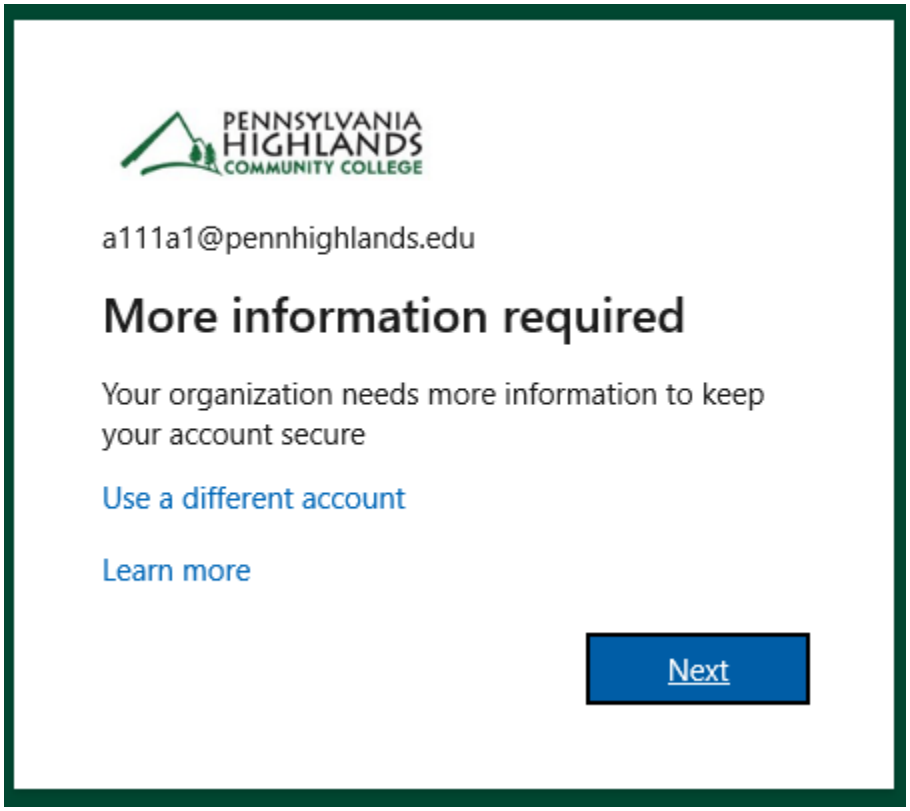
Step 1 - Change your Password

Change your password by entering your temporary password, providing a new password, and then confirming your new password entry.

Note: Your Penn Highlands account password requires you to have at least 8 characters, that are both upper and lower case, and must include numbers and/or special characters. Your password cannot contain any part of your name, and you may not repeat any of your last 5 passwords.



More information is required to activate your account. Click **Next** and follow the steps on the next page to set up your security profile for your Penn Highlands account.



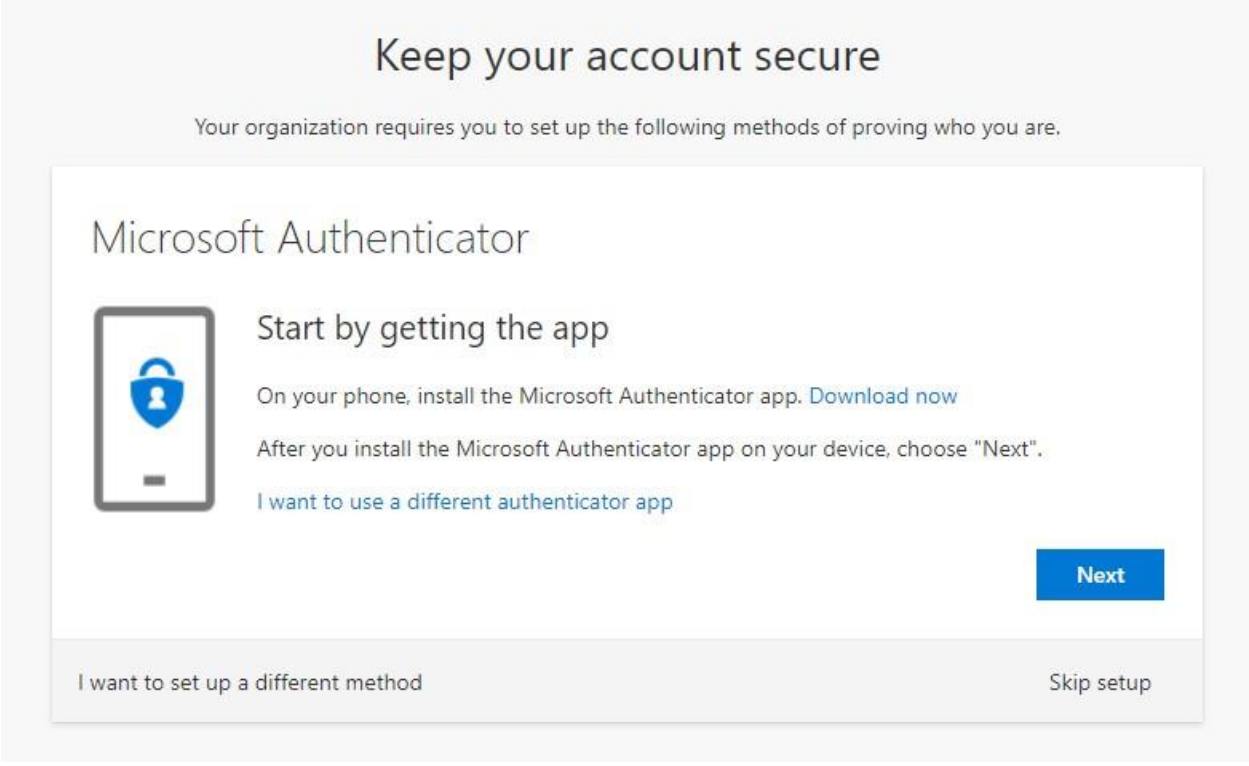
Step 2 - Set up your security profile using the wizard

To setup your security profile you will need to supply at least one method of identity verification, but we recommend setting up as many as methods that are available to you. This way if one of the methods is not available to you, you can refer to one of the other methods to confirm your identity. Additionally, you will already be set up for advanced security features like Multi-Factor Authentication (MFA), when that feature is made available.

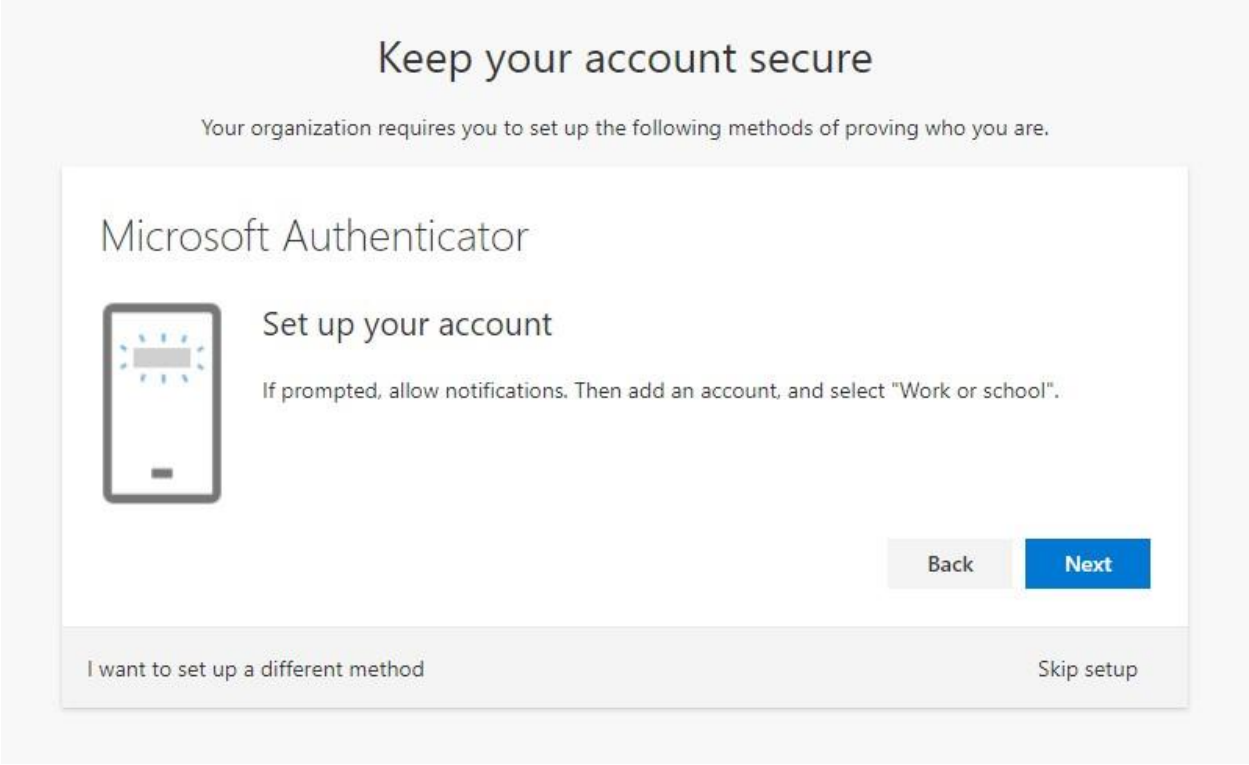
1. After you select **Next** from the prompt, a **Keep your account secure wizard** appears, showing the preferred method for you to set up, which is the Microsoft Authenticator app.

Note: If you want to use an authenticator app other than the Microsoft Authenticator app, select the **I want to use a different authenticator app** such as DUO or Google Authenticator. When using these alternative authenticator apps, you will only be able to generate a code that you must enter. You will not receive notification messages on your device like you do with the Microsoft Authenticator App.

If you want to choose a different method besides the authenticator app, you can select the **I want to set up a different method link**.



2. If you have not already downloaded the Microsoft Authenticator app on your mobile device, please do so now and then select **Next**.

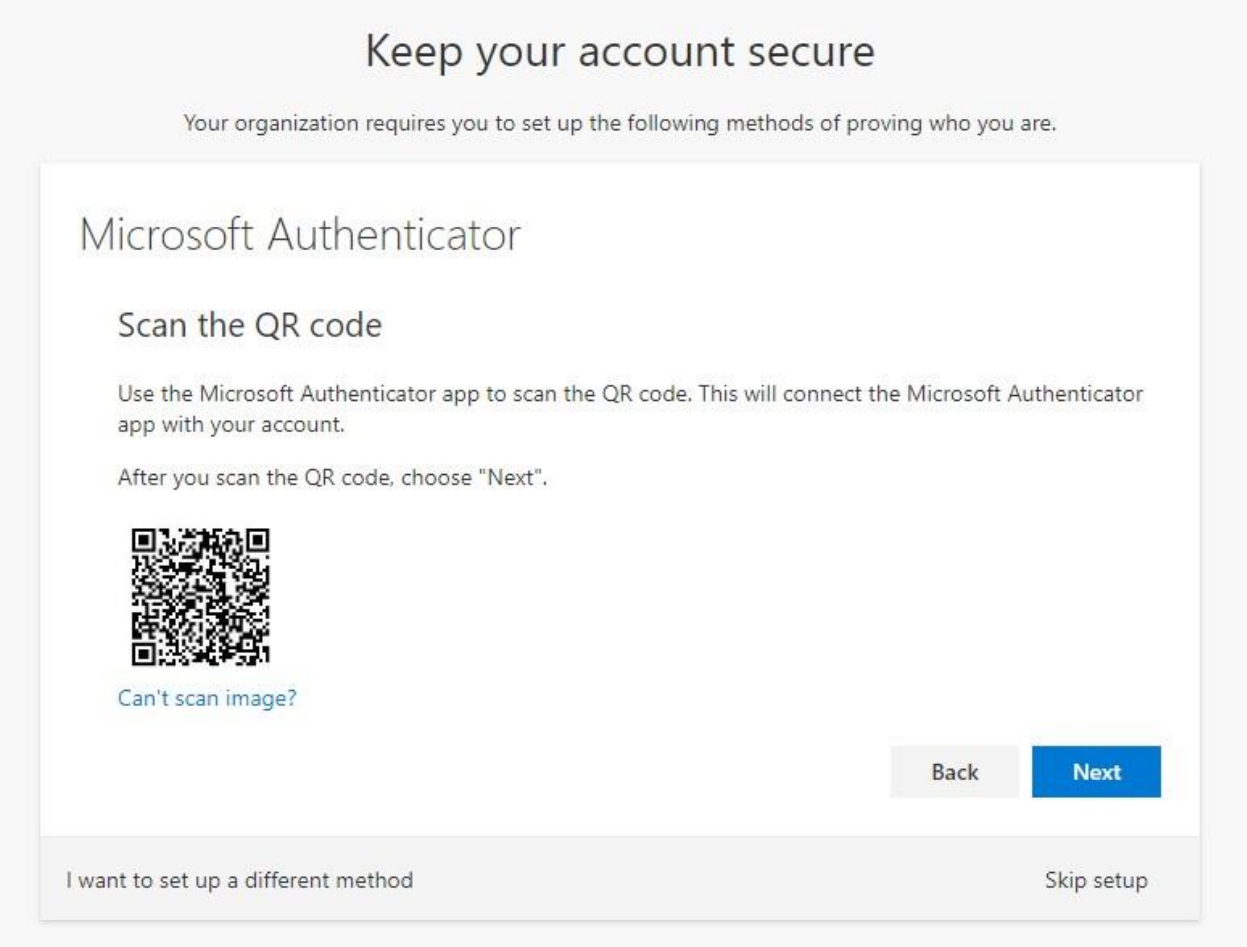


3. Remain on the **Set up your account** page while you set up the Microsoft Authenticator app on your mobile device.
4. Open the Microsoft Authenticator app, select to **allow notifications** (if prompted), select **Add account** from the **Customize and control** icon on the upper-right, and then select **Work or school account**.

Note: If this is the first time, you're setting up the Microsoft Authenticator app, you might receive a prompt asking whether to allow the app to access your camera (iOS) or to allow the app to take pictures and record video (Android). You must select **Allow** so the authenticator app can access your camera to take a picture of the QR code in the next step. If you don't allow the camera, you can still set up the authenticator app, but you'll need to add the code information manually.

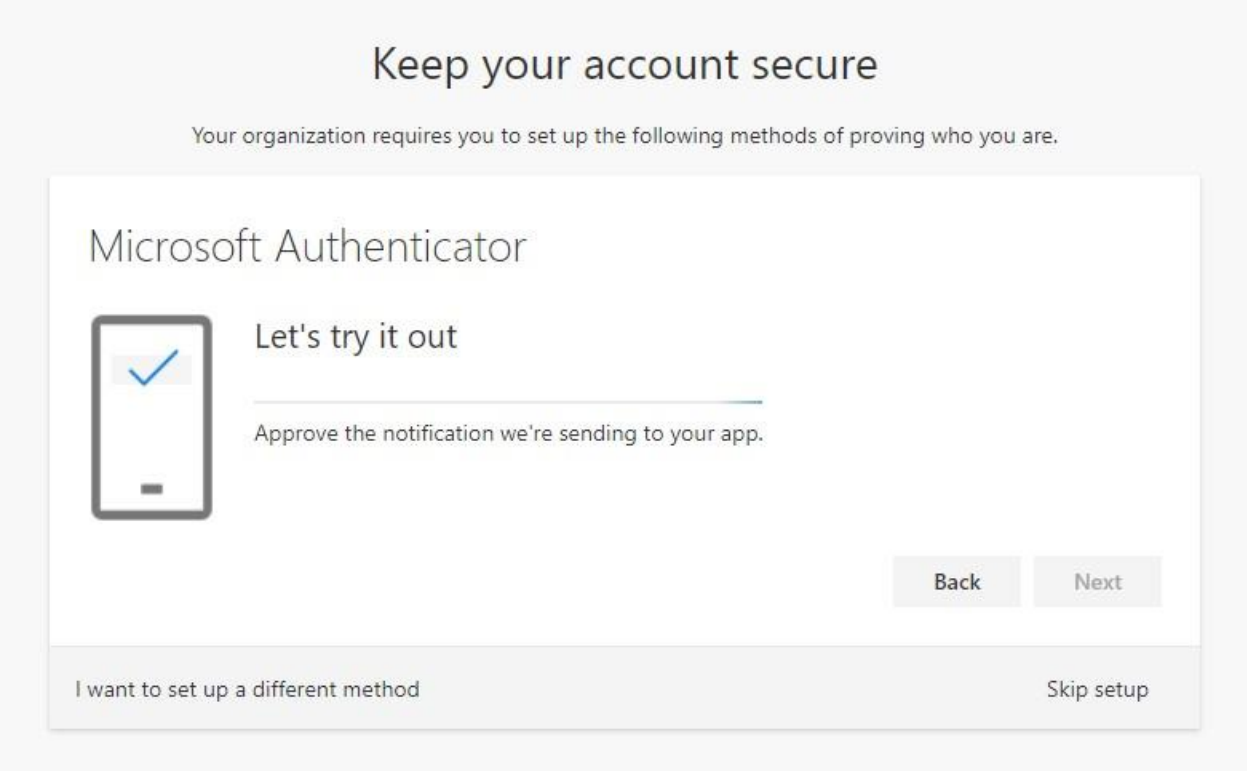
5. Return to the **Set up your account** page on your computer, and then select **Next**.

The **Scan the QR code** page appears.

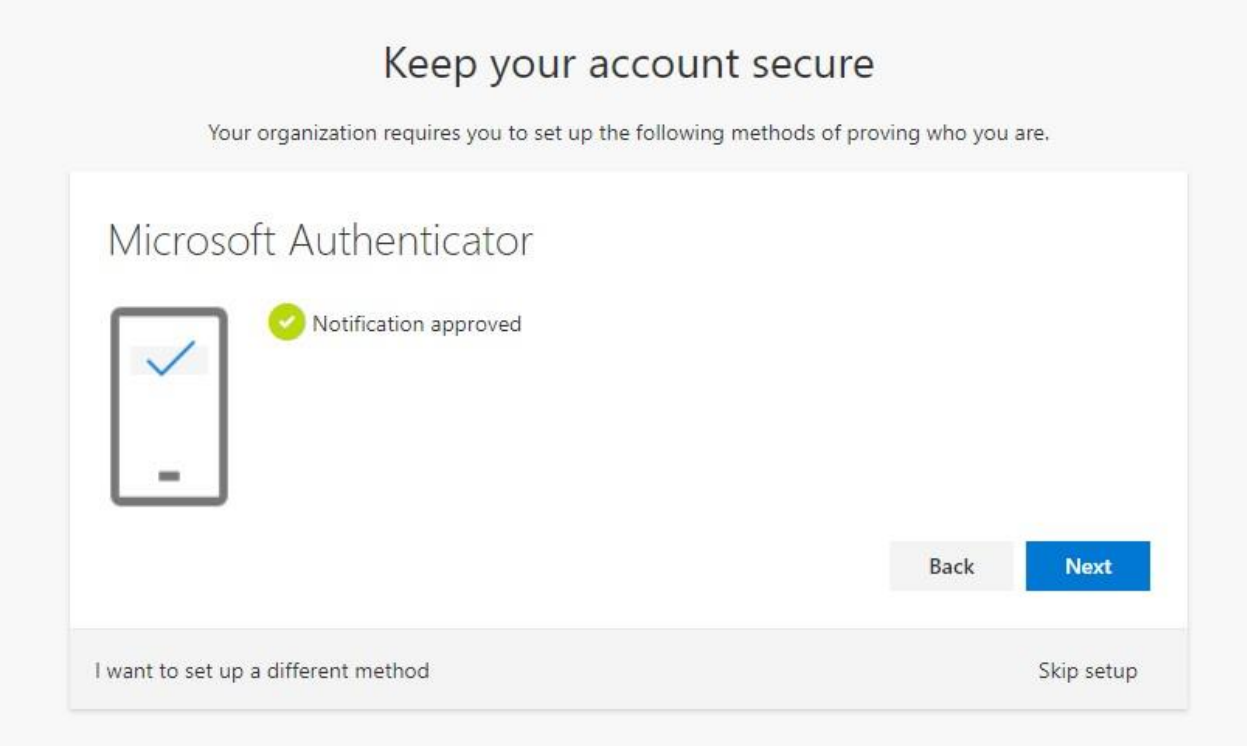


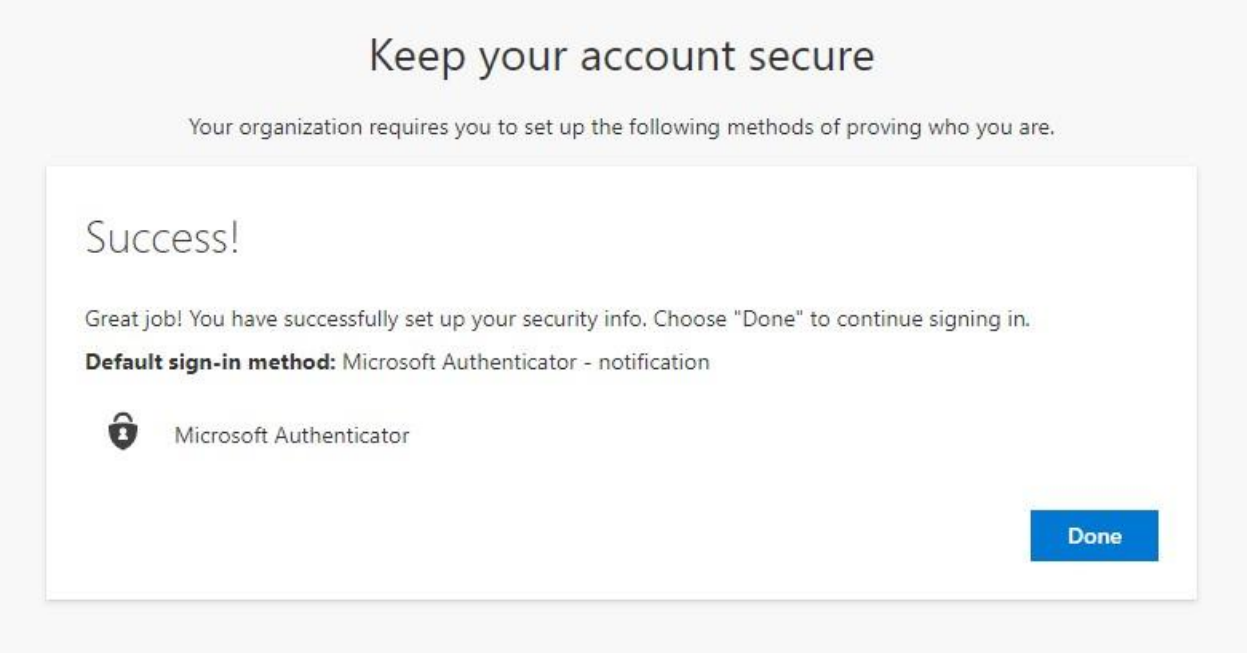
6. Scan the provided QR code with the Microsoft Authenticator app. The authenticator app should successfully add your work or school account without requiring any additional information from you. However, if the QR code reader can't read the code, you can select the **Can't scan the QR image** and manually enter the code and URL into the Microsoft Authenticator app.
7. Select **Next** on the **Scan the QR code** page on your computer.

A notification is sent to the Microsoft Authenticator app on your mobile device, to test your account.



8. Approve the notification in the Microsoft Authenticator app, and then select **Next**.

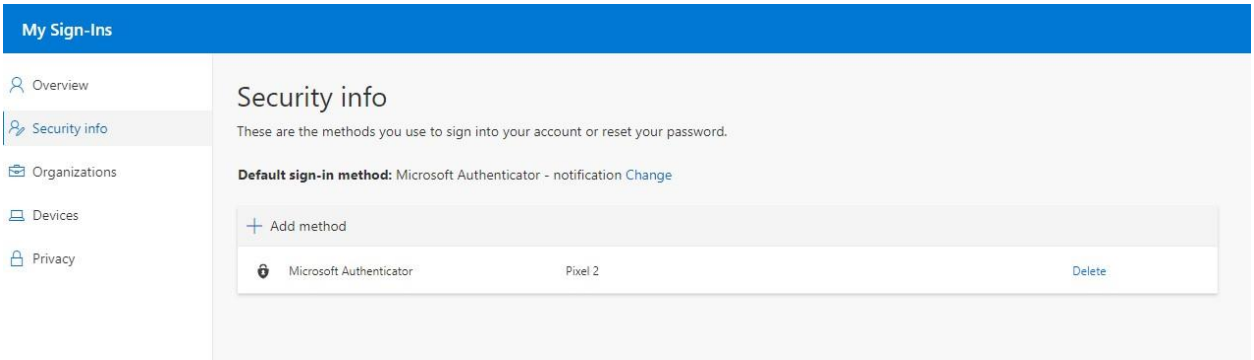


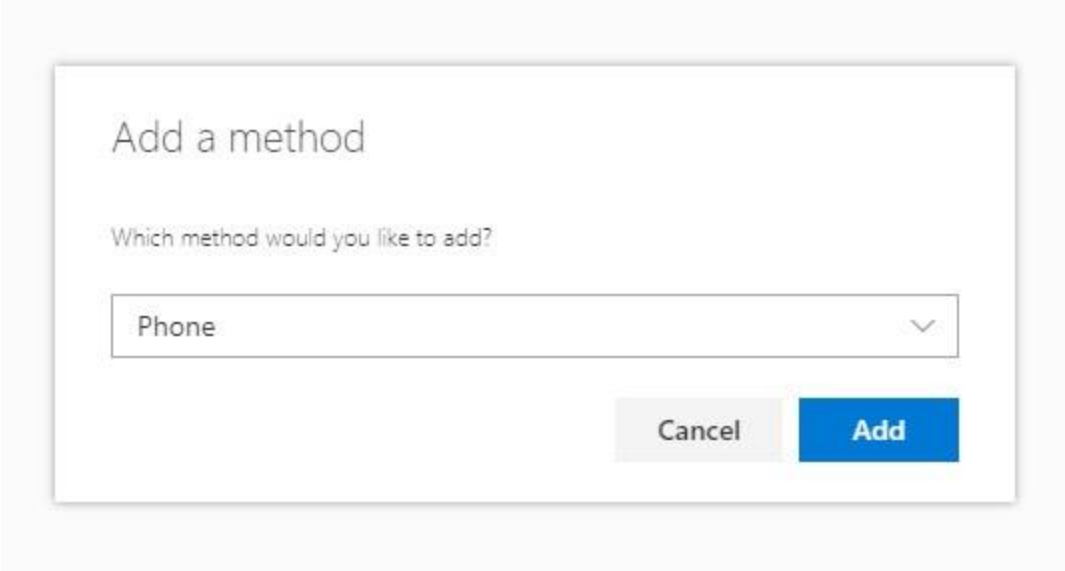


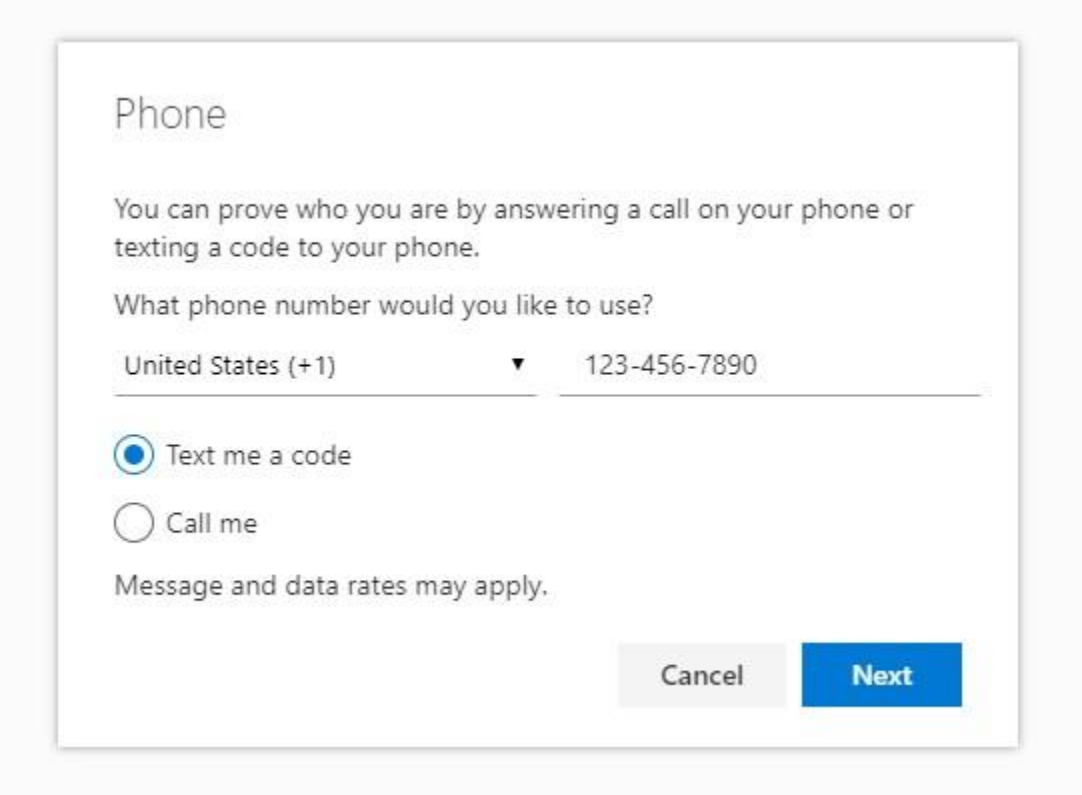
Your security info is updated to use the Microsoft Authenticator app by default to verify your identity when using two-step verification or password reset.

You should be returned to your **Security Info** Page, if not browse to https://aka.ms/mysecurityinfo.

9. To add additional verification methods, click on **Add method**. Select **Phone** from the drop-down list. This will take you to the **Phone** set up page, you must choose whether you want to receive a text message or a phone call, and then select **Next**. We suggest using text messages, so you must use a phone number for a device that can accept text messages.
   Note: You will get the chance to set up another phone number to receive a call on in the latter steps of this process.

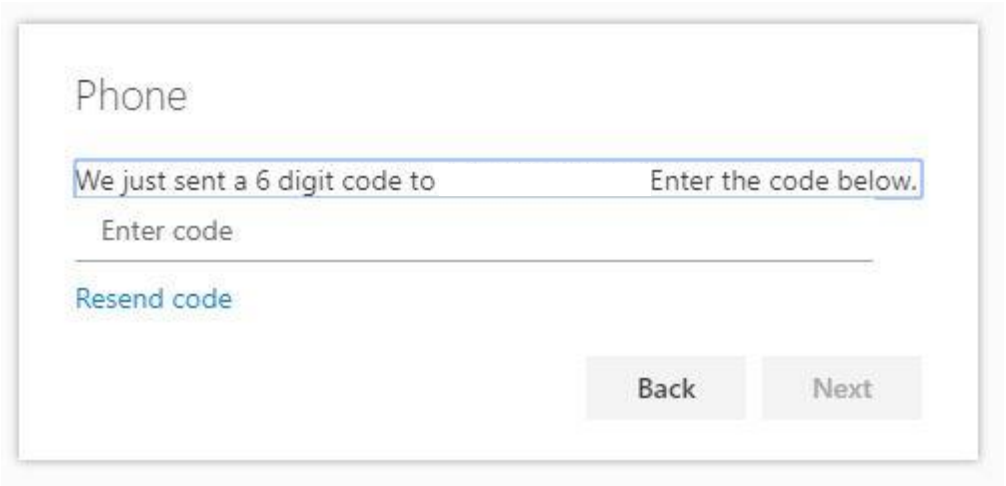


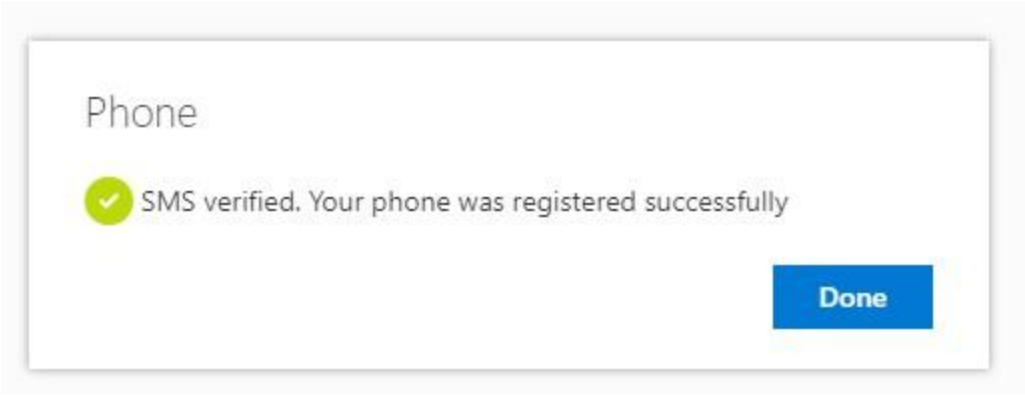




A text message is sent to your phone number. If would prefer to get a phone call, the process is the same. However, you'll receive a phone call with instructions, instead of a text message.

10. Enter the code provided by the text message sent to your mobile device, and then select **Next**.

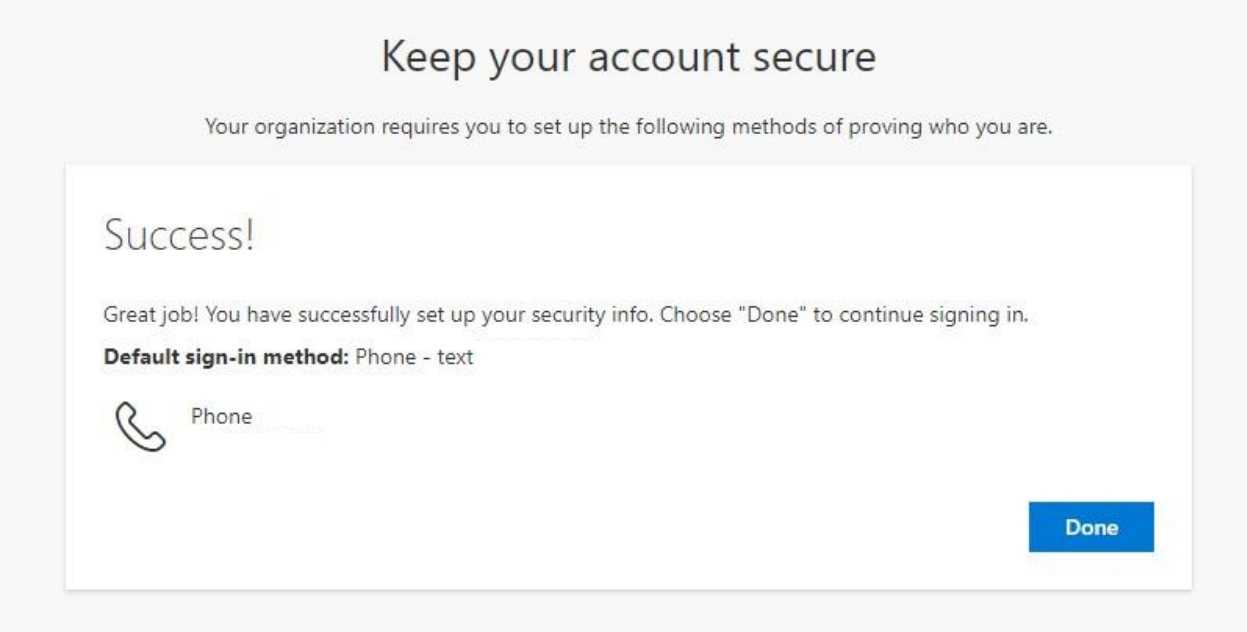




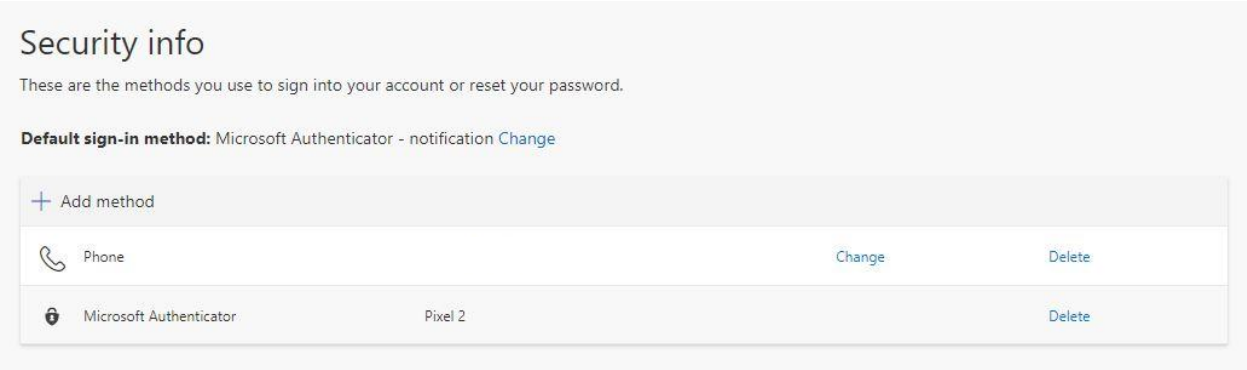
11. Review the success notification, and then select **Done**.

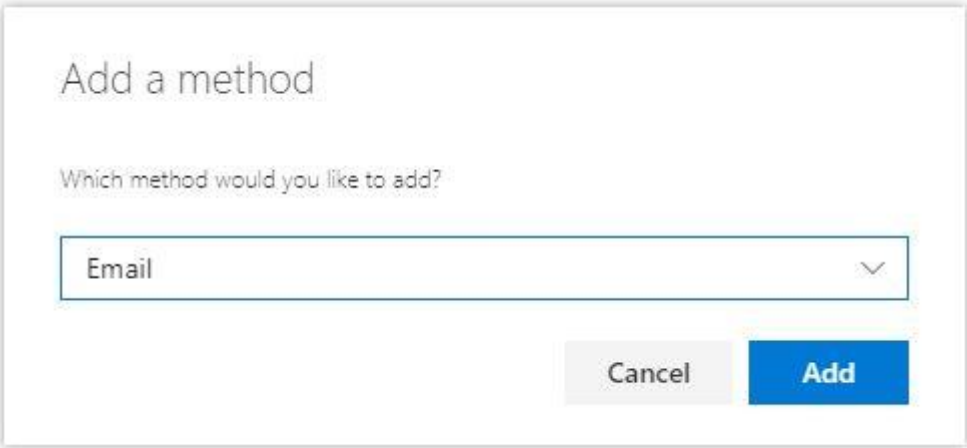
Your security info is updated to use text messaging as a backup method to verify your identity when using two-step verification or password reset.

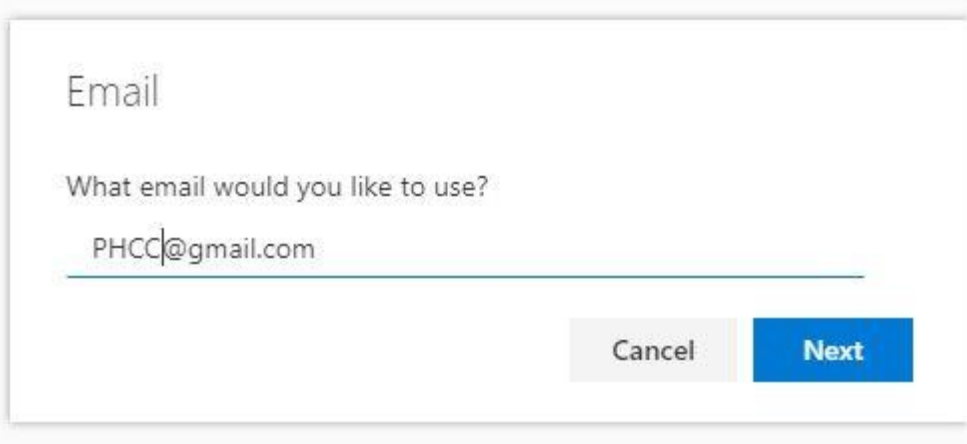
12. Review the **Success** page to verify that you've successfully set up both the Microsoft Authenticator app and a phone (text message) method for your security info, and then select **Done**.



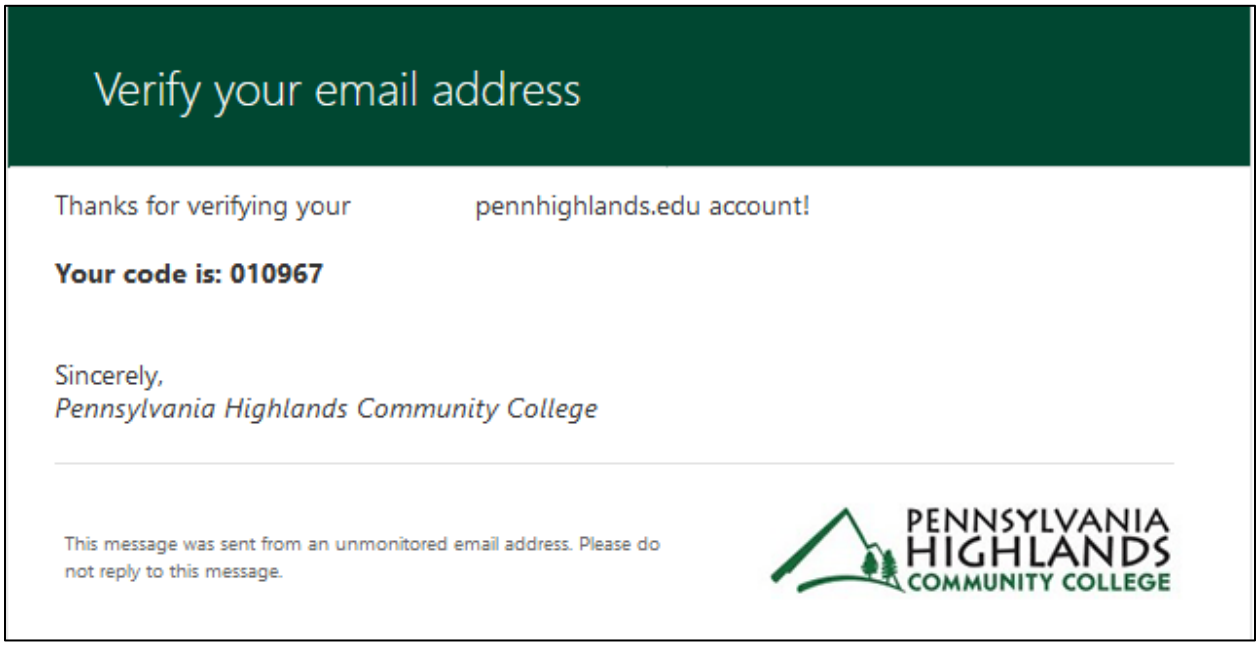
13. To add additional verification methods, click on **Add method**. Select **Email** from the drop-down list. This will take you to the **Email** set up page, where you must enter the email address of where you would like the verification notice sent, and then select **Next**. We suggest using a personal email address that you will have access to for this option.

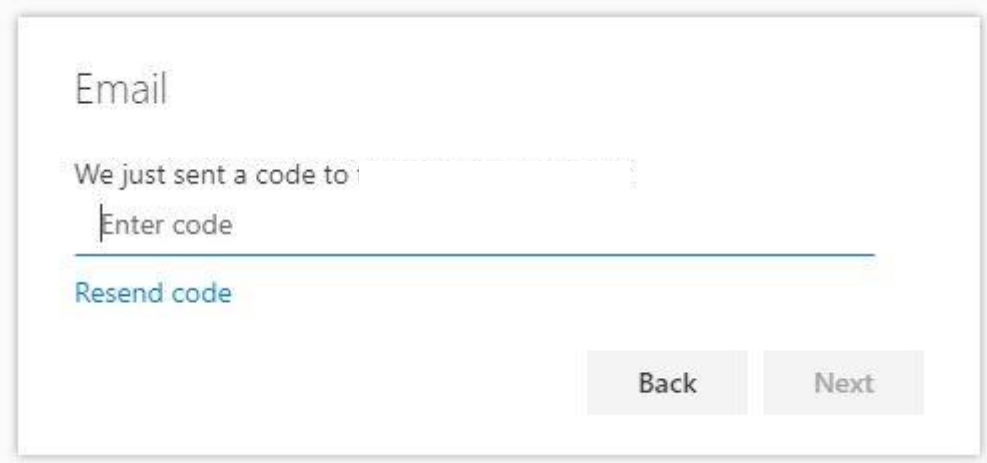






An email message is sent to the email address you specified. Enter the code provided in the email message, and then select **Next**.

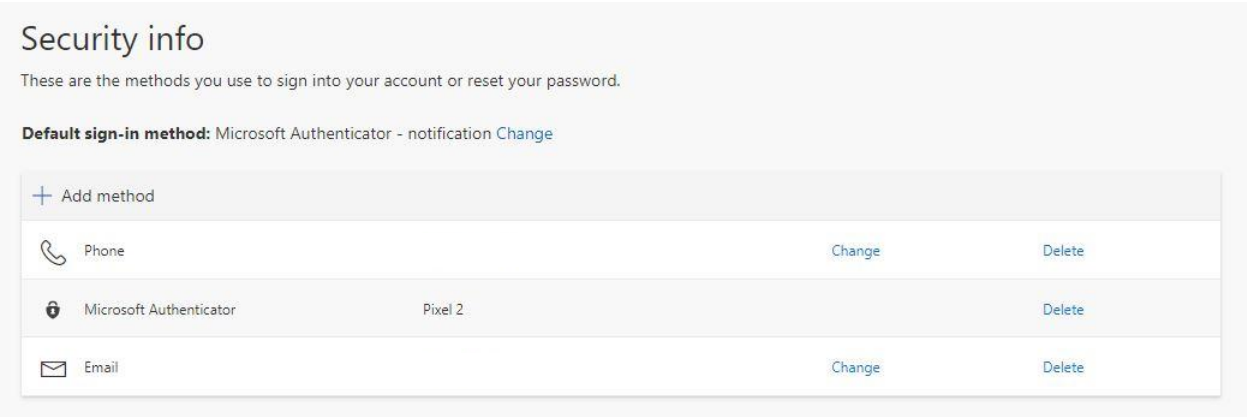




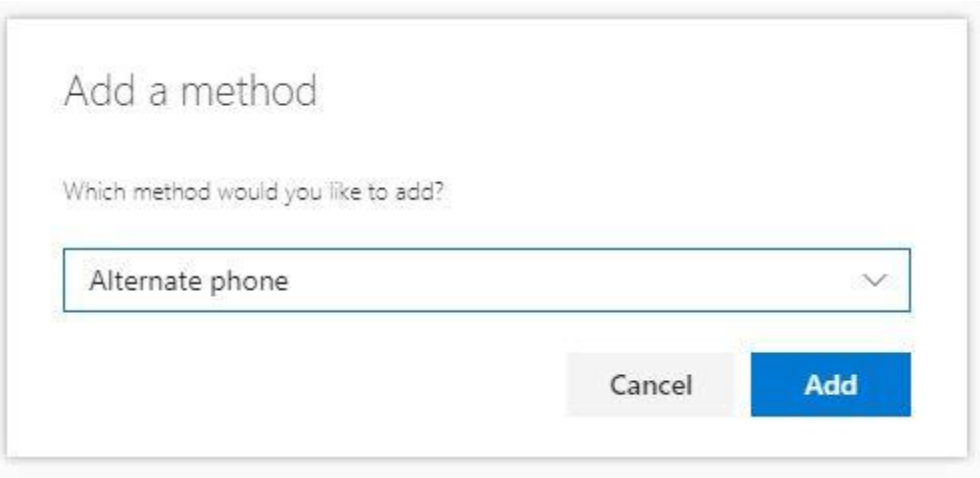
14. Review the success notification, and then select **Done**.

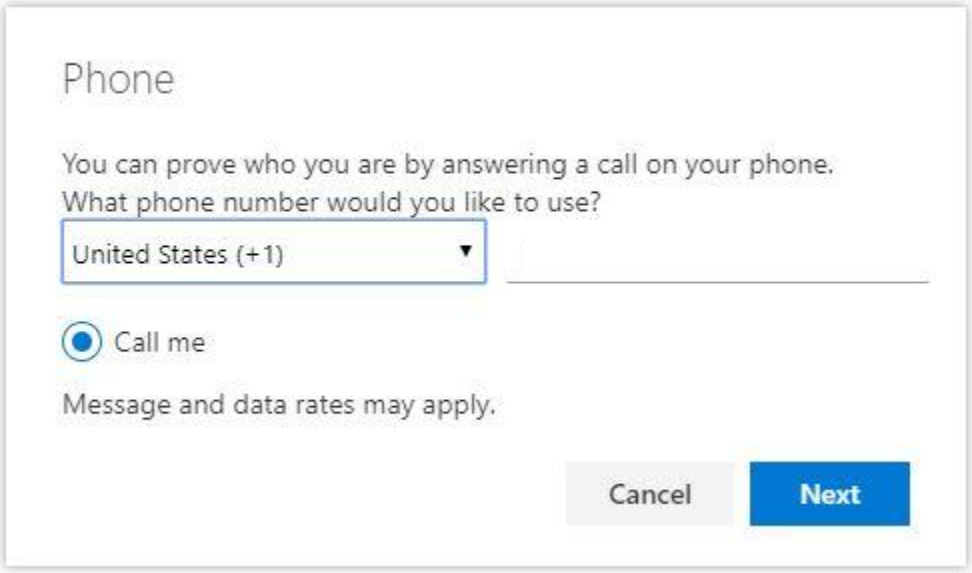
Your security info is updated to use an email message as a backup method to verify your identity when using two-step verification or password reset.

15. Review the **Success** page to verify that you've successfully set up both the Microsoft Authenticator app, phone (text message), and email as methods for your security info, and then select **Done**.

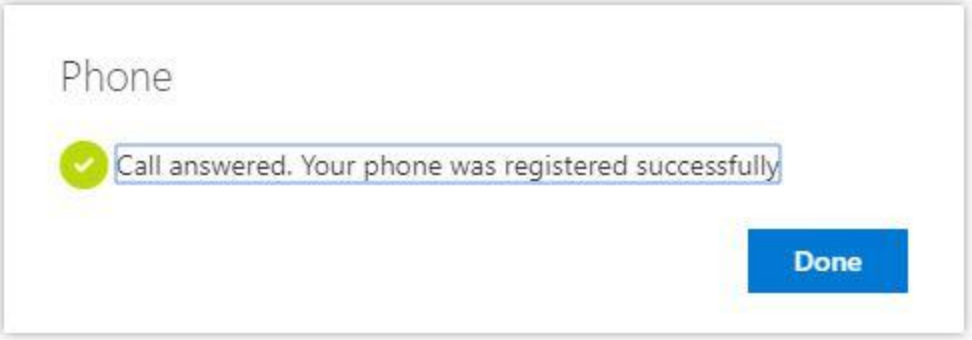


To add additional verification methods, click on **Add method**. Select **Alternate phone** from the drop-down list. This will take you to the **Phone** set up page, where you must enter a phone number of where you would like to receive the phone call to verify your identification and then select **Next**. We suggest using your home or office phone number for this method. Make sure you can answer the call for this method when setting it up. If you do not have access to this phone, you can always add it anytime by browsing to https://aka.ms/mysecurityinfo and run through the add Alternate Phone method.



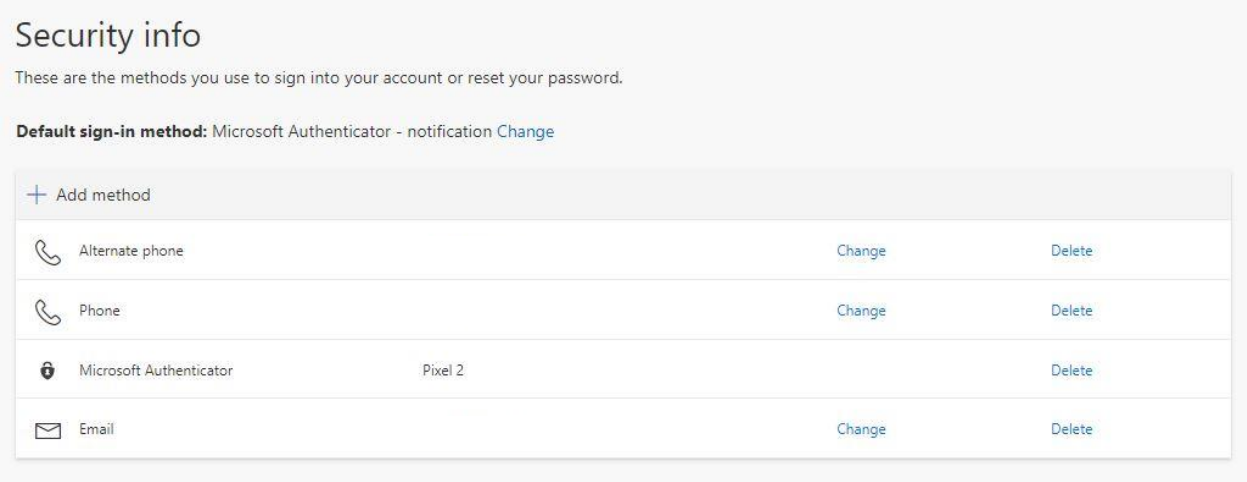


A phone call is made to the specified phone number. Press the # key to verify your identity, and then select **Next**.



16. Review the success notification, and then select **Done**.

Your security info is updated to use an alternate phone number as a backup method to verify your identity when using two-step verification or password reset.



17. Review the **Success** page to verify that you've successfully set up both the Microsoft Authenticator app, phone (text message), email, and an alternative phone as methods for your security info, and then select **Done**.

Note: Make sure you adjust the **Default sign-in method** to your preferred method, otherwise it will default to the last method added. Your list may vary depending on the methods you added or if you used a different Authenticator App.

Click on **Change** and pick your preferred method from the dropdown:

1. **Microsoft Authenticator App – Notification**
2. **Microsoft Authenticator App – Code**
3. **Phone – Text (**Mobile Phone Number**)**
4. **Phone – Call (**Mobile Phone Number**)**
5. **Phone – Call (**Alternate Phone Number**)**