

Secure your Penn Highlands account with Multi-Factor Authentication (MFA)

After you sign-in to your Penn Highlands Office 365 account, you can follow these steps below when you're prompted to set up your security info. This will allow you to enhance the security on your Pennsylvania Highlands Office 365 account by allowing for the verification of your identity while logging in to your account.

Note: If you have previously set up Self-service Password reset for your Office 365 account, then you do not need to do anything further as you have already supplied your identity verification information. If you would like to review your change your security information, please see visit <https://aka.ms/mysecurityinfo>.

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.

Multi-Factor Authentication (MFA) registration requires enrollment of at least 1 mobile device such as a phone, tablet, and/or another hardware device. To enroll you can 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.

You can use the Microsoft Authenticator app in multiple ways, including:

- Verify your identify when trying to reset your password.
- Respond to a prompt for authentication after you sign in with your username and password.

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

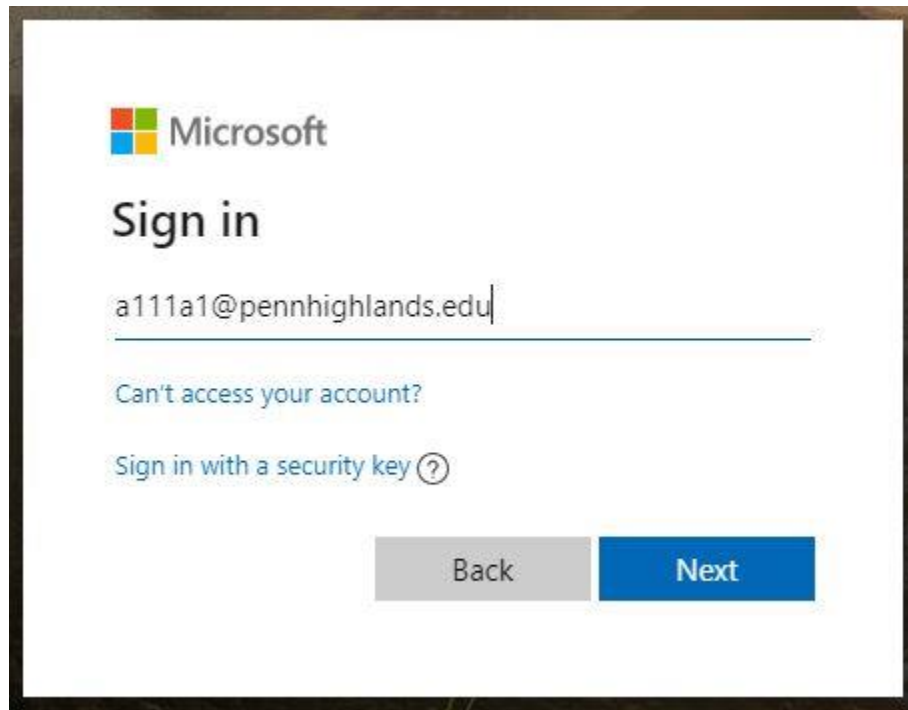


<https://apps.apple.com/us/app/microsoft-authenticator/id983156458>

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>.

Sign-in to your Penn Highlands account

After you sign-in to your Penn Highlands account, you'll see a prompt that asks you to provide more information before it lets you access your account.





← a111a1@pennhighlands.edu

Enter password

Password

[Forgot my password](#)

Sign in



a111a1@pennhighlands.edu

More information required

Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

Next

Set up your security info using the wizard

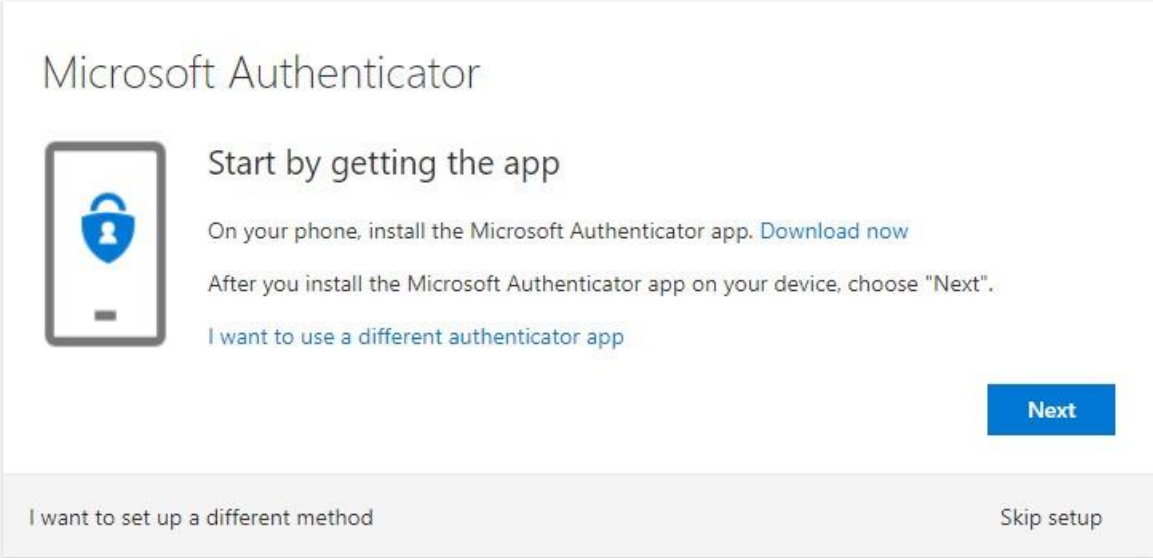
Follow these steps to set up your security info for your Penn Highlands account from the “**More Information Required**” prompt.

To setup Multi-Factor Authentication (MFA) you need to supply at least one method, 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.

1. After you select **Next** from the prompt, a **Keep your account secure wizard** appears, showing the first method your administrator and organization require you to set up. For this example, it's 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**.

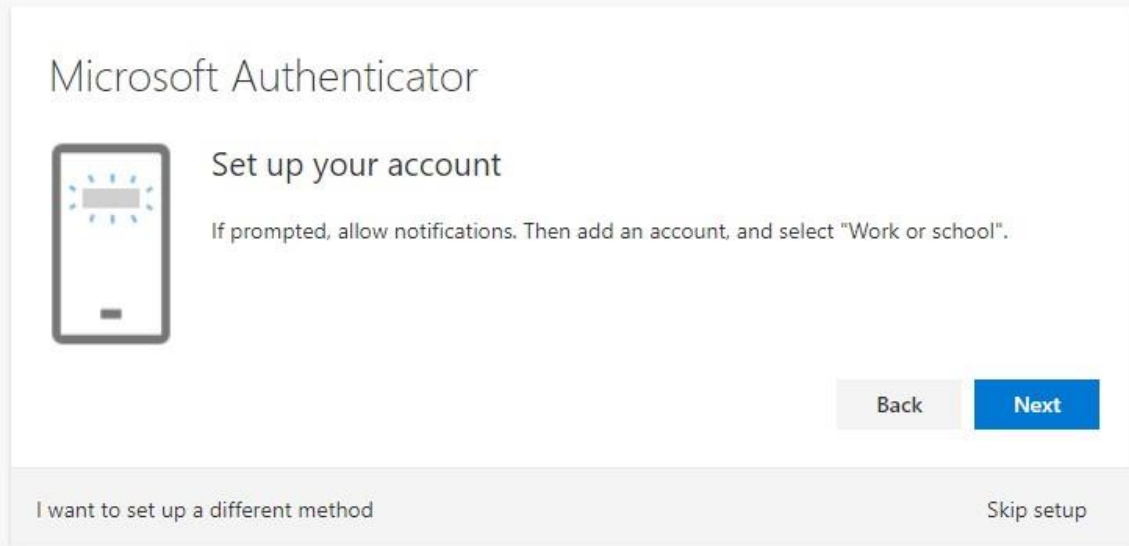


The screenshot shows a wizard titled "Keep your account secure" with the subtitle "Your organization requires you to set up the following methods of proving who you are." The main heading is "Microsoft Authenticator". To the left is an icon of a smartphone with a blue shield and a person silhouette. The text says "Start by getting the app". Below this, it says "On your phone, install the Microsoft Authenticator app. [Download now](#)". Then, "After you install the Microsoft Authenticator app on your device, choose 'Next'." There is a link: "[I want to use a different authenticator app](#)". At the bottom right is a blue "Next" button. At the bottom left is a link: "[I want to set up a different method](#)". At the bottom right is a link: "[Skip setup](#)".

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

Keep your account secure

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

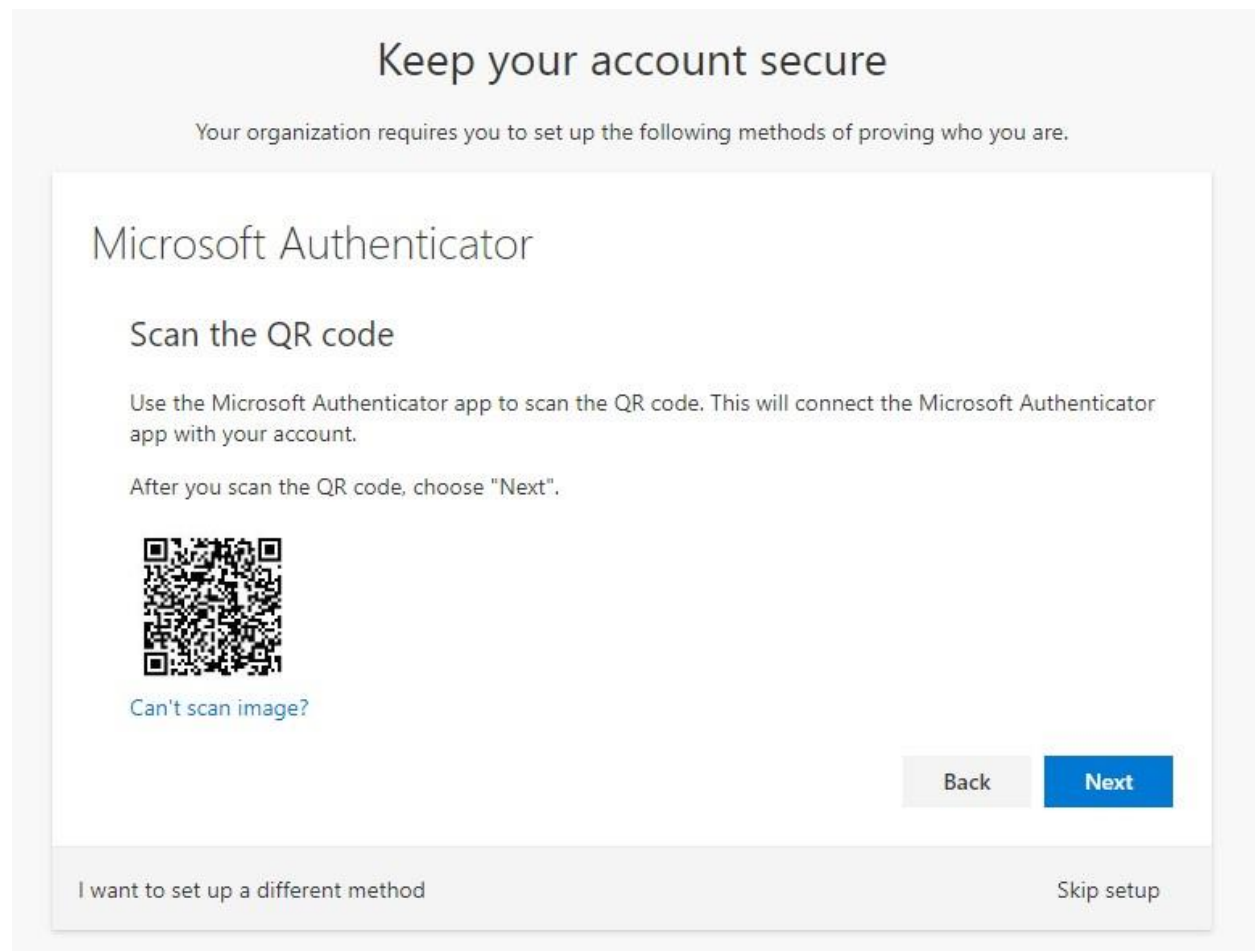


3. Remain on the **Set up your account** page while you set up the Microsoft Authenticator app on your mobile device.
4. Open the Microsoft Authenticator app, select to allow notifications (if prompted), select **Add account** from the **Customize and control** icon on the upper-right, and then select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

Keep your account secure

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

Microsoft Authenticator



Let's try it out

Approve the notification we're sending to your app.

Back

Next

I want to set up a different method

Skip setup

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

Keep your account secure

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

Microsoft Authenticator



✔ Notification approved

Back

Next

I want to set up a different method

Skip setup

Keep your account secure

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

Success!

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

Default sign-in method: Microsoft Authenticator - notification



Microsoft Authenticator

Done

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.

My Sign-Ins

- Overview
- Security info
- Organizations
- Devices
- Privacy

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](#)

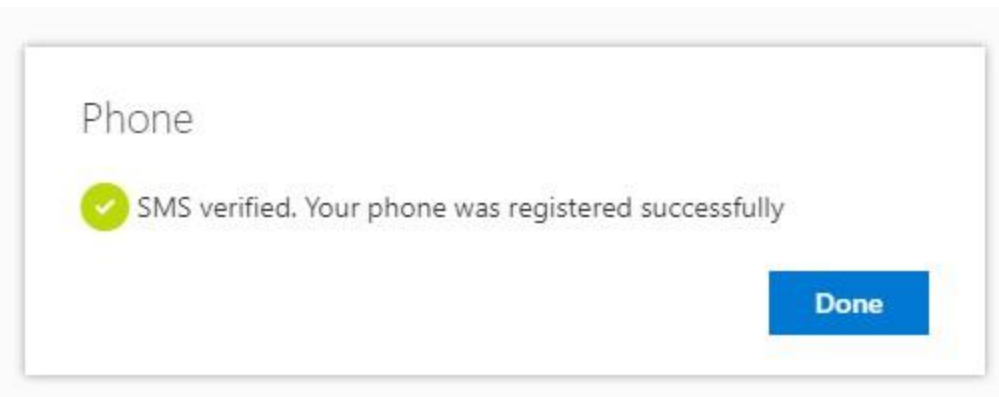
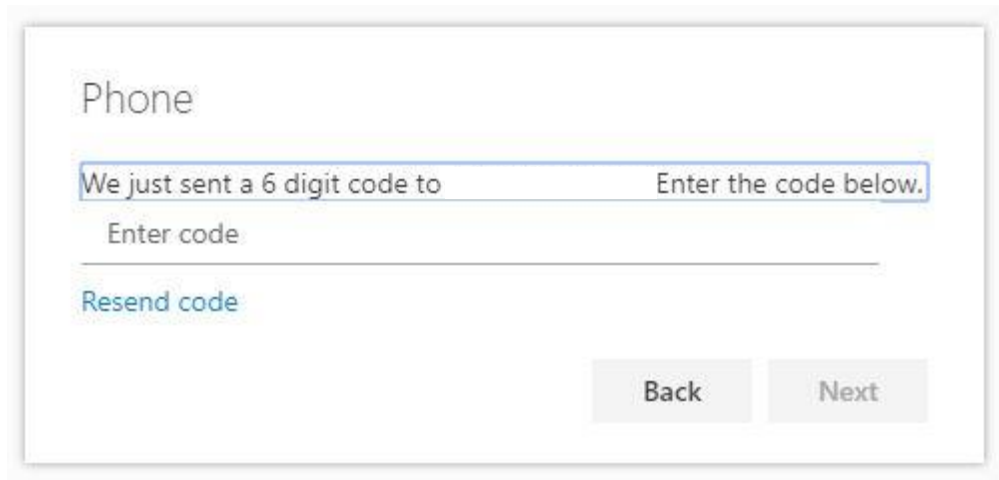
+ Add method

Microsoft Authenticator	Pixel 2	Delete
-------------------------	---------	------------------------

The image shows two sequential screenshots of a mobile application interface. The first screenshot, titled "Add a method", asks the user "Which method would you like to add?". A dropdown menu is open, showing "Phone" as the selected option. Below the dropdown are two buttons: "Cancel" and "Add". The second screenshot, titled "Phone", provides instructions: "You can prove who you are by answering a call on your phone or texting a code to your phone." It then asks "What phone number would you like to use?". A dropdown menu shows "United States (+1)" and a text input field contains "123-456-7890". Below this are two radio button options: "Text me a code" (which is selected) and "Call me". A note states "Message and data rates may apply." At the bottom are "Cancel" and "Next" buttons.

A text message is sent to your phone number. If you 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 (either text message or phone call) method for your security info, and then select **Done**.


Keep your account secure

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

Success!

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

Default sign-in method: Phone - text

 Phone

[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.

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	Change	Delete
 Microsoft Authenticator	Pixel 2	Delete

Add a method

Which method would you like to add?

Email

Cancel Add

Email

What email would you like to use?

PHCC@gmail.com

Cancel Next

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

Verify your email address

Thanks for verifying your pennhighlands.edu account!

Your code is: 010967

Sincerely,
Pennsylvania Highlands Community College

This message was sent from an unmonitored email address. Please do not reply to this message.



Email

We just sent a code to

Enter code

[Resend code](#)

Back

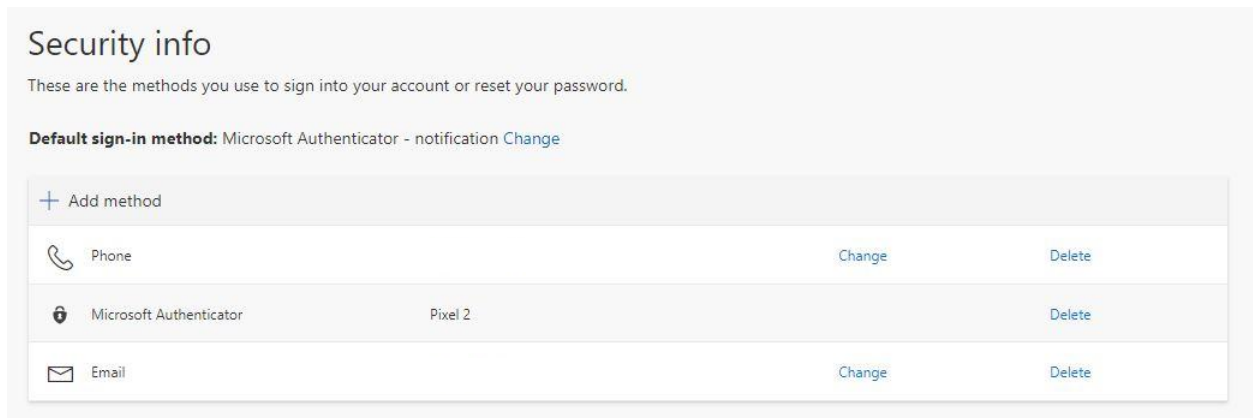
Next

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

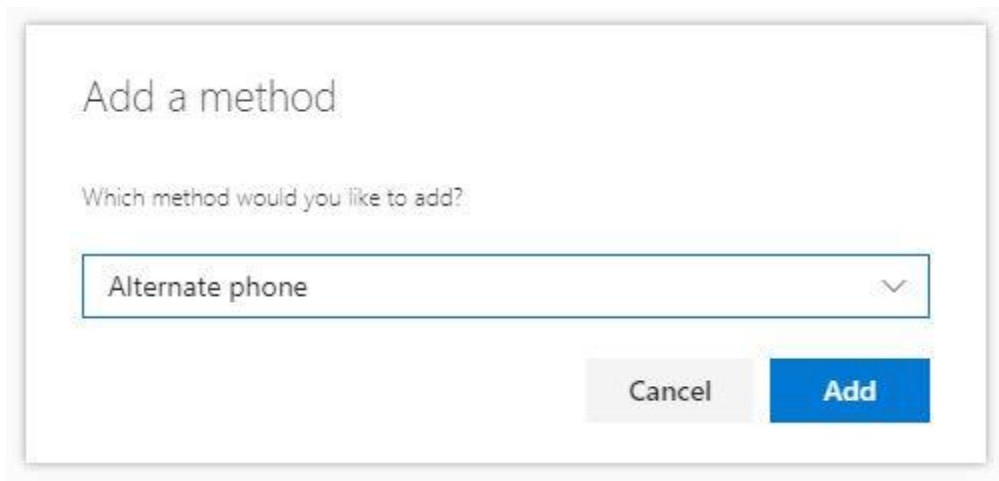
Your security info is updated to use an email message as a backup method to verify your identity when using two-step verification or password reset.

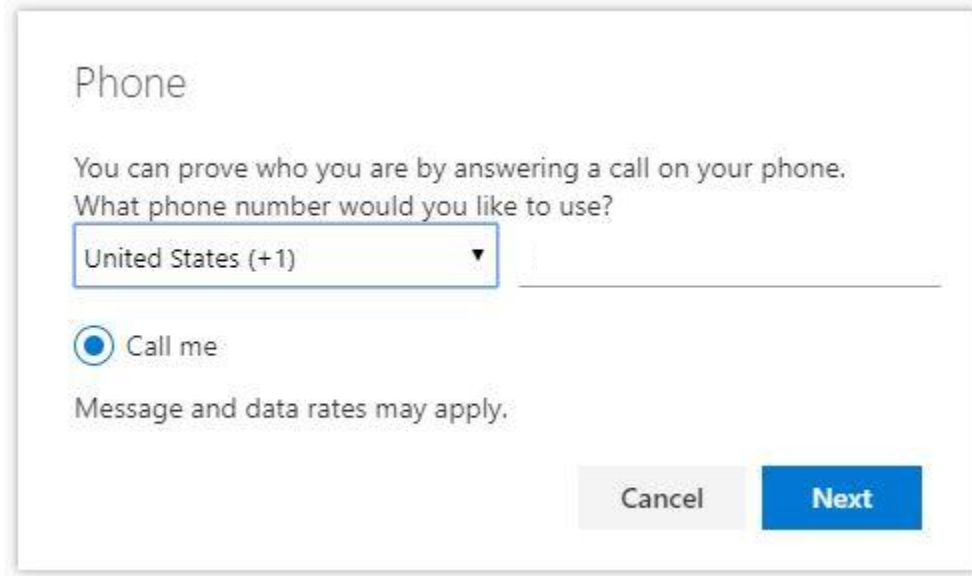
15. Review the **Success** page to verify that you've successfully set up both the Microsoft Authenticator app, phone (text message), and email as methods for your security info,

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.





Phone

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

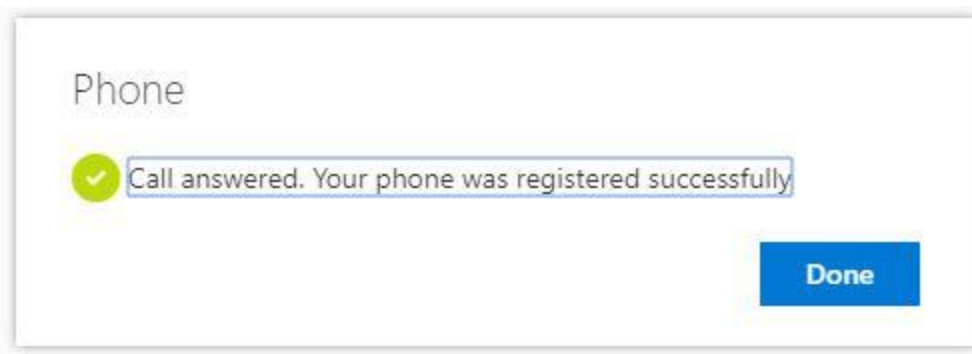
United States (+1)

Call me

Message and data rates may apply.

Cancel Next

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



Phone

Call answered. Your phone was registered successfully

Done

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.

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			
	Alternate phone	Change	Delete
	Phone	Change	Delete
	Microsoft Authenticator	Pixel 2	Delete
	Email	Change	Delete

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)**