



# Multi-Factor Authentication (MFA) Guide

Updated 05/08/2026

## About

**Multi-factor authentication (MFA)** is a method of authentication that requires your password and an **additional verification method**, such as a code or token.

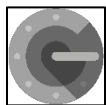
Below are instructions for how to set up Multi-Factor Authentication (MFA) for your Single Sign-on (SSO) login. **The approved methods for MFA are:**



[SMS Text Message](#)



[Microsoft Authenticator](#)



[Google Authenticator](#)



[Phone Call](#)



[Hardware Token](#)

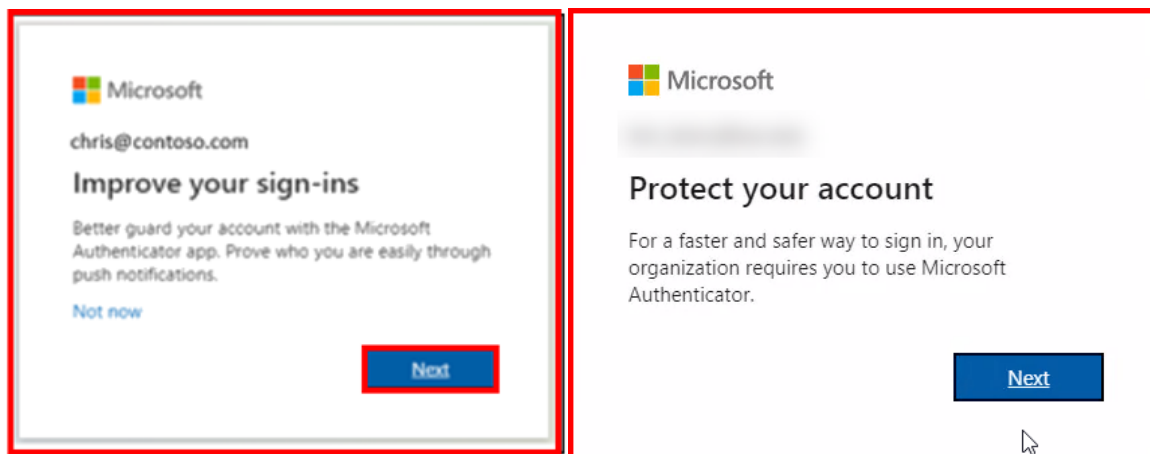
**ITS strongly recommends for you to setup and [manage your backup authentication methods.](#)**

## 09/15/23 - Important Changes when using SMS Text or Phone Call

**NOTE:** On September 15 2023, Microsoft will begin prompting users who authenticate using [SMS Text Message](#) and [phone call](#) to set up the [Microsoft Authenticator](#) when they sign into their work or school account.

You can select **“Not now”** to skip the **“Improve your sign-ins”** prompt up to 3 times, but after that, you will be forced to set up Microsoft Authenticator at the **“Protect your account”** screen.

Please follow the instructions for how to use [Microsoft Authenticator](#) if you are prompted to **Improve your sign-ins** or **Protect your account**.

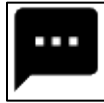


# Table of Contents

ABOUT..... 1

09/15/23 - IMPORTANT CHANGES WHEN USING SMS TEXT OR PHONE CALL..... 2

TABLE OF CONTENTS..... 3



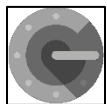
**SMS TEXT MESSAGE..... 5**

STEP 1 – LOGIN TO MICROSOFT WEBSITE..... 5  
STEP 2 – A PROMPT APPEARS TO “IMPROVE YOUR SIGN-INS” OR “MORE INFORMATION REQUIRED.” ..... 5  
STEP 2 – SELECT “I WANT TO SET UP A DIFFERENT METHOD”, THEN SELECT PHONE. .... 6  
STEP 3 – ENTER PHONE NUMBER, THEN SELECT “TEXT ME A CODE” ..... 6  
STEP 4 – ENTER VERIFICATION CODE SENT THROUGH SMS TEXT TO YOUR PHONE ..... 7  
STEP 5 – COMPLETE SETUP AND OFFICE.COM LOGIN ..... 8  
STEP 6 - VERIFY YOUR IDENTITY WITH SMS TEXT MESSAGE ON NEXT LOGIN ..... 9



**MICROSOFT AUTHENTICATOR ..... 10**

STEP 1 – DOWNLOAD THE MICROSOFT AUTHENTICATOR APP. .... 10  
STEP 2 – SIGN INTO YOUR MICROSOFT ACCOUNT ..... 11  
STEP 3 – A PROMPT APPEARS TO “IMPROVE YOUR SIGN-INS” OR “MORE INFORMATION REQUIRED.” ..... **ERROR! BOOKMARK NOT DEFINED.**  
STEP 4 - AT “KEEP YOUR ACCOUNT SECURE” SCREEN, MAKE SURE YOU HAVE THE MICROSOFT AUTHENTICATOR APP ALREADY INSTALLED ON YOUR PHONE. .... 11  
STEP 5 - FOLLOW THE PROMPTS TO “SET UP YOUR ACCOUNT.” ..... 13  
STEP 6 - SCAN THE QR CODE DISPLAYED ON THE MICROSOFT WEBSITE. .... 14  
*If you initiated MFA setup from your phone instead of a computer: ..... 15*  
STEP 7 – FOLLOW THE “LET’S TRY IT OUT” PROMPTS..... 16  
STEP 8 – COMPLETE SETUP AND OFFICE.COM LOGIN ..... 17  
STEP 9 - VERIFY YOUR IDENTITY WITH MICROSOFT AUTHENTICATOR ON NEXT LOGIN ..... 18



**GOOGLE AUTHENTICATOR ..... 19**

STEP 1 – LOGIN TO MICROSOFT WEBSITE..... 19  
STEP 2 – A PROMPT APPEARS TO “IMPROVE YOUR SIGN-INS” OR “MORE INFORMATION REQUIRED.” ..... **ERROR! BOOKMARK NOT DEFINED.**  
STEP 3 – SELECT “I WANT TO SET UP A DIFFERENT AUTHENTICATOR APP..... 20  
STEP 4 – DOWNLOAD AND INSTALL THE GOOGLE AUTHENTICATOR APP ..... 21  
STEP 5 – SET UP YOUR ACCOUNT AND SCAN THE QR CODE ..... 22  
STEP 6 – VERIFY THE GOOGLE AUTHENTICATOR APP WORKS..... 25  
STEP 7 – COMPLETE SETUP AND OFFICE.COM LOGIN ..... 26  
STEP 8 - VERIFY YOUR IDENTITY WITH GOOGLE AUTHENTICATOR ON NEXT LOGIN..... 27



**PHONE CALL..... 28**

STEP 1 – LOGIN TO MICROSOFT WEBSITE..... 28

STEP 2 – A PROMPT APPEARS TO “IMPROVE YOUR SIGN-INS” OR “MORE INFORMATION REQUIRED.” ..... **ERROR! BOOKMARK NOT DEFINED.**

STEP 3 – SELECT “I WANT TO SET UP A DIFFERENT METHOD”, THEN SELECT PHONE. .... 28

STEP 4 – ENTER PHONE NUMBER, THEN SELECT “CALL ME” ..... 29

STEP 5 – ANSWER THE PHONE CALL FROM MICROSOFT AND PRESS # KEY TO VERIFY. .... 30

STEP 6 – COMPLETE SETUP AND OFFICE.COM LOGIN ..... 31

STEP 7 – VERIFY YOUR IDENTITY WITH PHONE CALL ON NEXT LOGIN ..... 32



**HARDWARE TOKEN..... 33**

STEP 1 – REQUEST A HARDWARE TOKEN FROM THE ITS DEPARTMENT ..... 33

STEP 2 – LOGIN TO OFFICE.COM WITH YOUR SINGLE SIGN-ON (SSO) USERNAME ..... 33

STEP 3 – ENTER THE VERIFICATION CODE ..... 33

STEP 4 – COMPLETE OFFICE.COM LOGIN ..... 34

STEP 5 - VERIFY YOUR IDENTITY WITH HARDWARE TOKEN ON NEXT LOGIN..... 34

**MANAGE YOUR BACKUP AUTHENTICATION METHODS..... 35**

STEP 1 – SIGN INTO HTTPS://AKA.MS/MFASETUP ..... 35

STEP 2 – ADD, DELETE, OR CHANGE YOUR SIGN-IN METHODS..... 36

STEP 3A - ADD A SIGN-IN METHOD ..... 37

STEP 3B - DELETE A SIGN-IN METHOD..... 38

STEP 3C - CHANGE DEFAULT SIGN-IN METHOD..... 39

STEP 3D - CHANGE AN EXISTING SIGN-IN METHOD ..... 40

STEP 3E - SIGN IN WITH AN ALTERNATIVE METHOD ..... 41

**TROUBLESHOOTING PROBLEMS ..... 42**

TROUBLESHOOTING SIGN-IN PROBLEMS ..... 42

TROUBLESHOOTING OTHER PROBLEMS ..... 42

RECEIVING HELP ..... 42



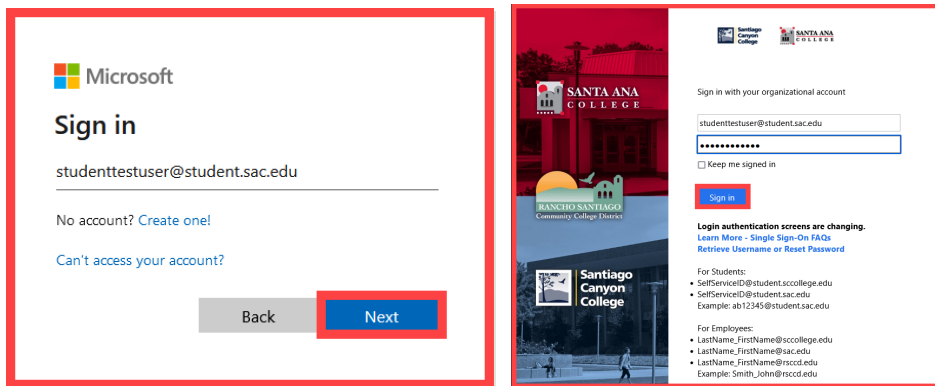
## SMS Text Message

**NOTE:** This requires a mobile device with a phone number that has SMS enabled.

### Step 1 – Login to Microsoft website

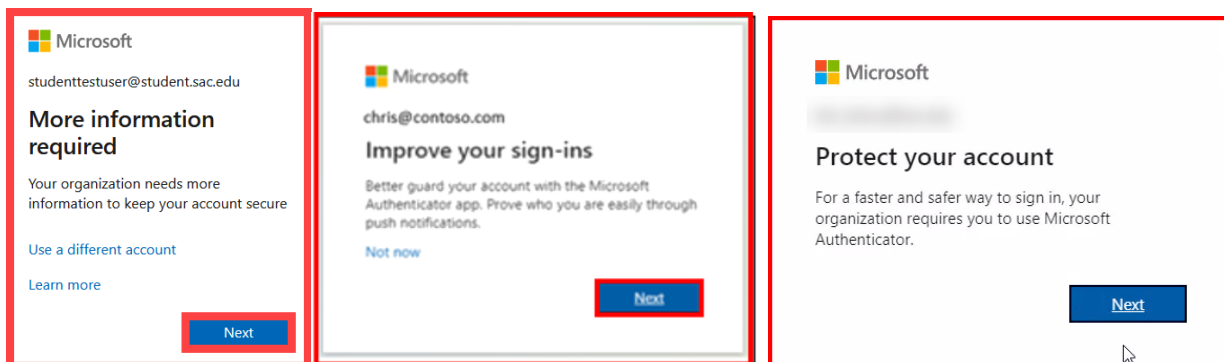
Go to [www.office.com](http://www.office.com) or Outlook Web Access at <https://outlook.office.com>.  
Sign into your account using your **Single Sign-On credentials**.

We recommend using a **desktop, laptop, or tablet**. Use Google Chrome or Microsoft Edge web browser for the best experience.



### Step 2 – A prompt appears for “More Information required,” “Improve your sign-ins,” or “Protect your account.”

Select **Next**. \*



\* **NOTE:** You can select “Not now” to skip the “**Improve your sign-ins**” prompt up to 3 times, but after that, you will be forced to set up Microsoft Authenticator.

## Step 2 – Select “I want to set up a different method”, then select Phone.

Select **I want to set up a different method**. Select **Phone**.

Keep your account secure

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

Microsoft Authenticator

Start by getting the app

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose "Next".

[I want to use a different authenticator app](#)

[Next](#)

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

Choose a different method ×

Which method would you like to use?

Phone

[Cancel](#) [Confirm](#)

## Step 3 – Enter phone number, then select “Text me a code”

Enter your **phone number** and select **Text me a code**. Select **Next**.

Keep your account secure

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

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?

United States (+1) 7146

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](#).

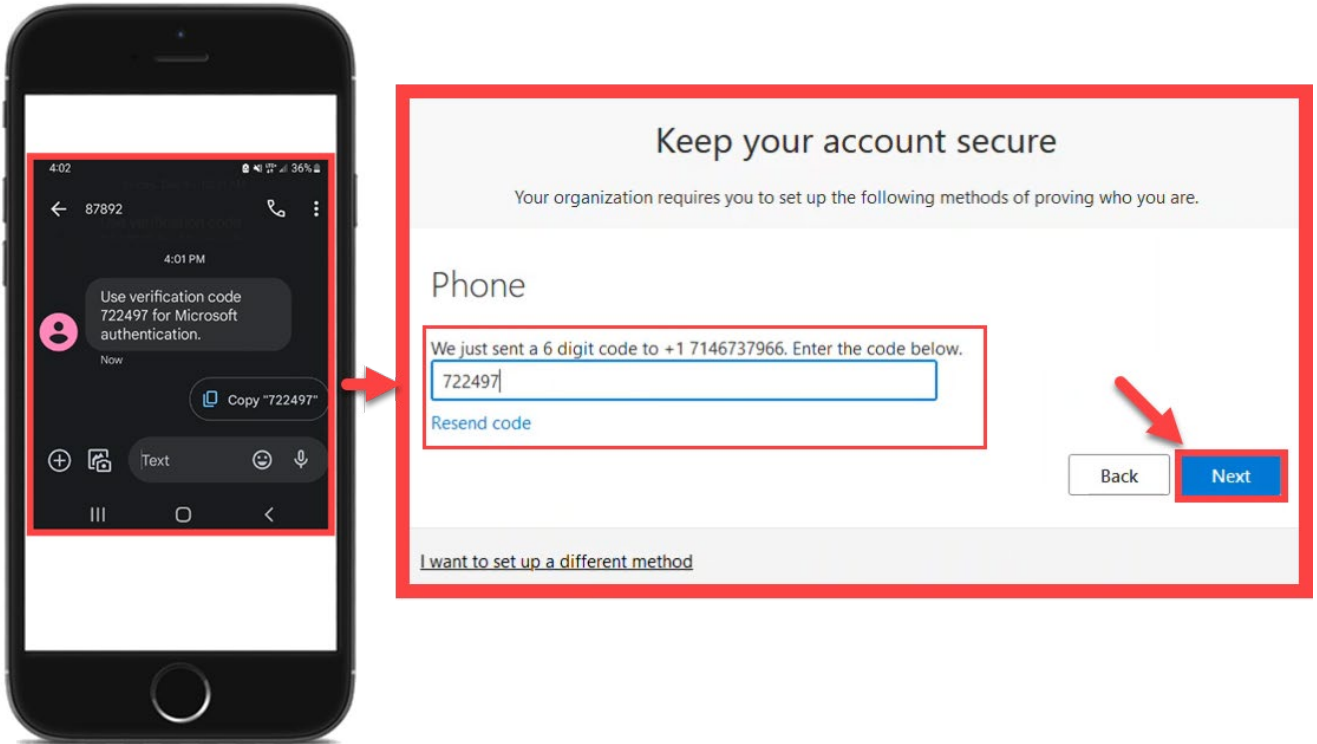
[Next](#)

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

## Step 4 – Enter verification code sent through SMS text to your phone

On your phone, check for a **verification code** sent from Microsoft, sent through **SMS Text message**.

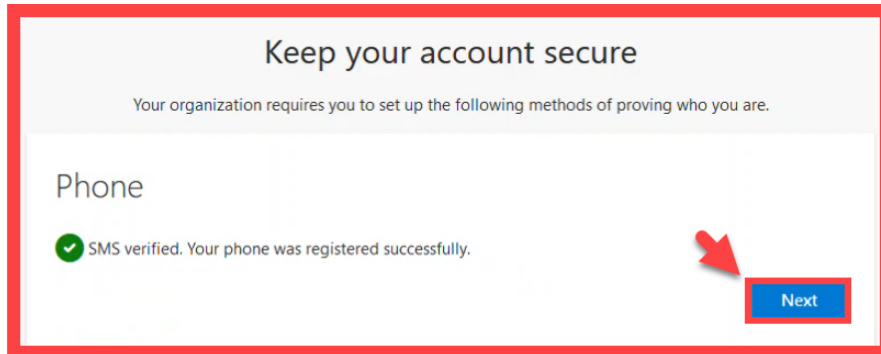
Enter the **verification code** on the website. Select **Next** to continue.



**NOTE:** If you receive an error message here, select **Resend code**. The verification code may have expired if it took too long to enter it.

## Step 5 – Complete setup and Office.com login

Select **Next** to continue.



Keep your account secure

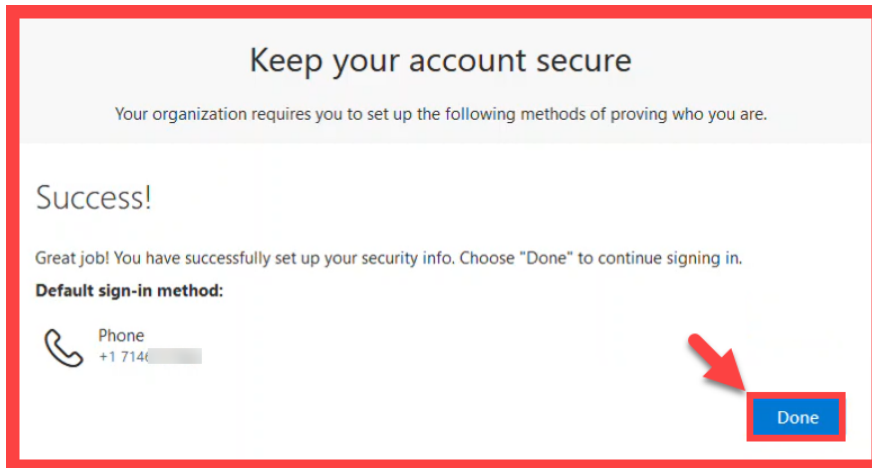
Your organization requires you to set up the following methods of proving who you are.

Phone

✔ SMS verified. Your phone was registered successfully.

Next

Select **Done** to finish the set up.



Keep your account secure

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

Success!

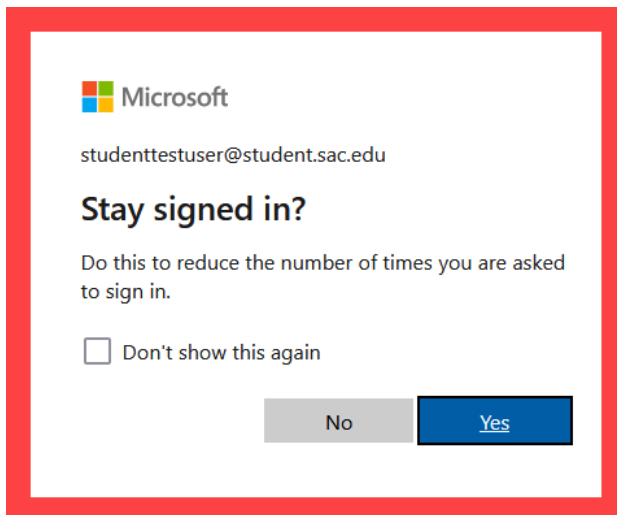
Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

**Default sign-in method:**

Phone  
+1 714...

Done

If prompted, select **Yes** or **No** for whether to **Stay signed in** with your account.



Microsoft

studenttestuser@student.sac.edu

**Stay signed in?**

Do this to reduce the number of times you are asked to sign in.

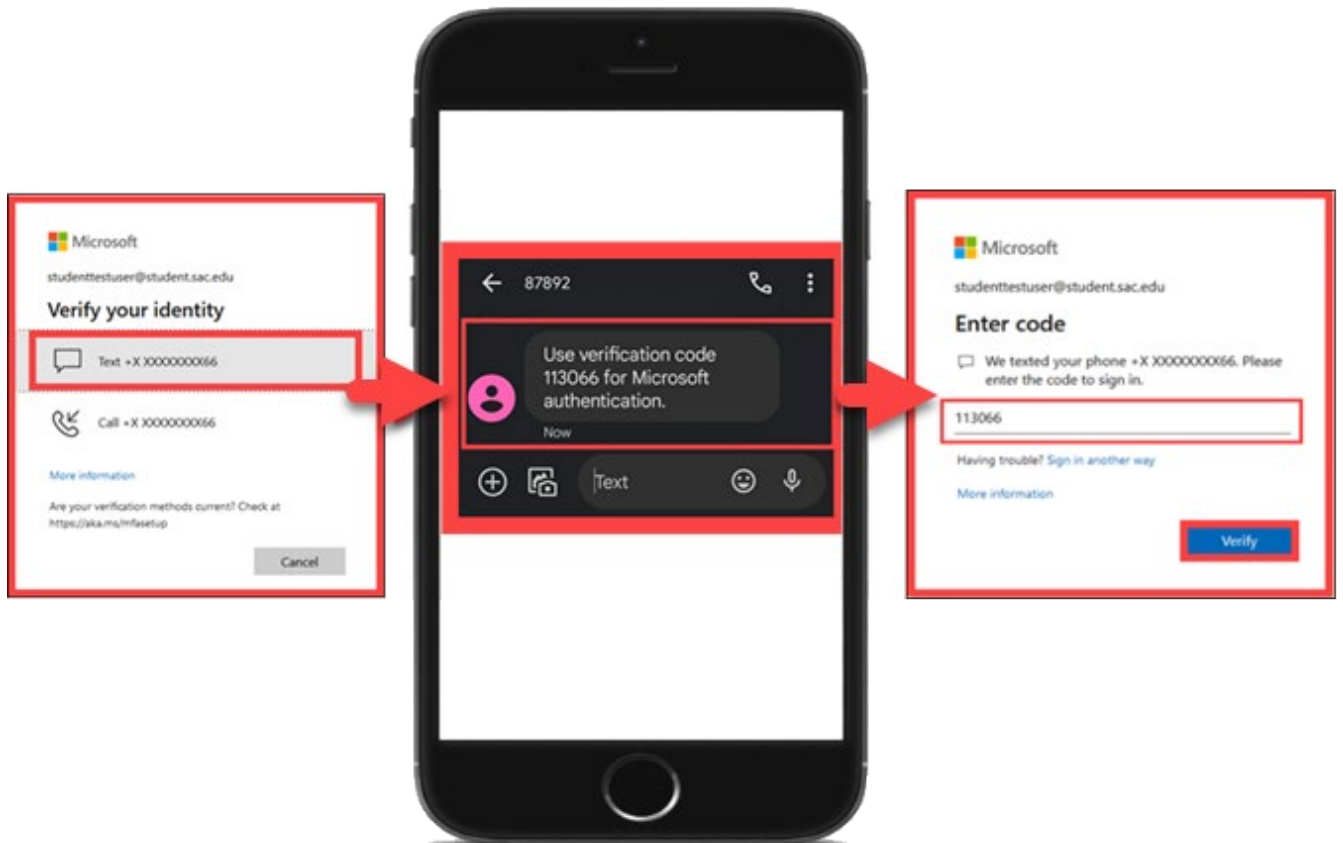
Don't show this again

No Yes

## Step 6 - Verify your identity with SMS Text Message on next login

The next time you login to and are prompted to **Verify your Identity**:

1. Select the **Text +X XXXXXXXXX** option.
2. **Check your mobile device for a text message from Microsoft.**
3. **Input the verification code.**
4. Select **Verify** to continue.



**NOTE: Only "Verify" SMS text message codes that you have initiated yourself.**

If you receive an unknown text prompting you to input a verification code that you did not initiate, ignore the prompt, and contact the [ITS Help Desk](#).



# Microsoft Authenticator

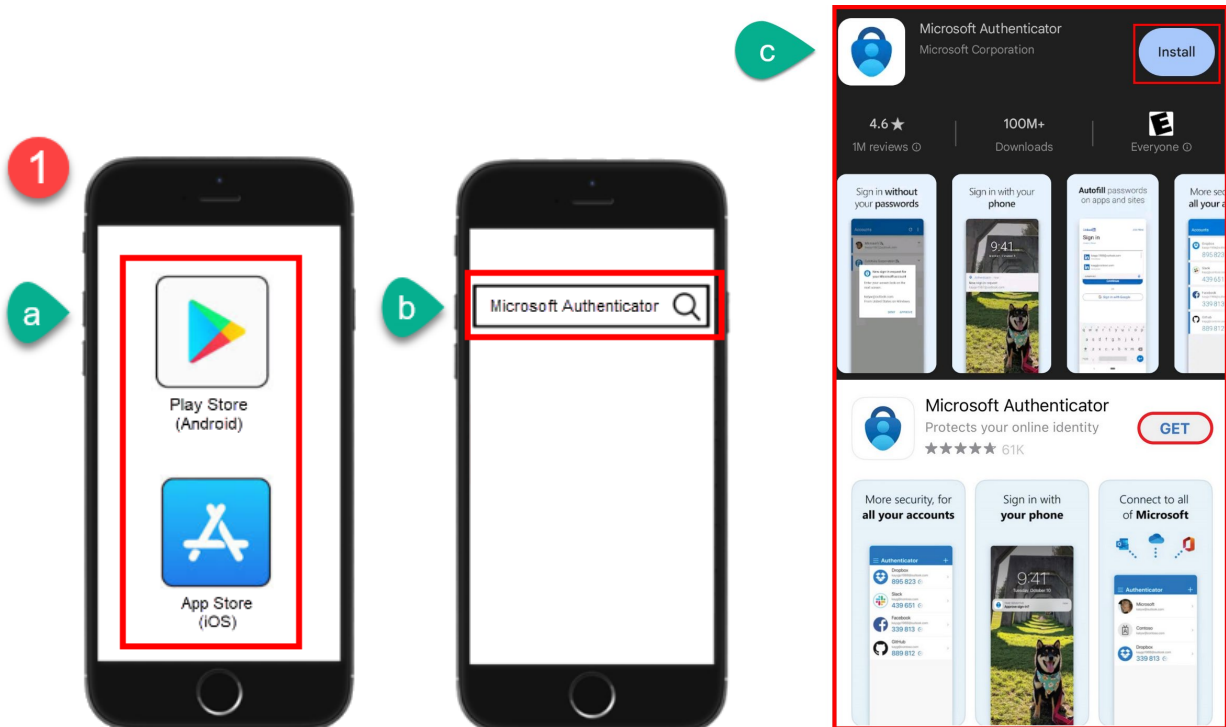
**NOTE:** This requires a mobile device with access to **Microsoft Authenticator app**.

## Step 1 – Download the Microsoft Authenticator app.

### How to download the Microsoft Authenticator app:

- a. On your phone, open the **App Store** or **Play Store**.
- b. Search for **Microsoft Authenticator**.
- c. **Install or Get** the **Microsoft Authenticator app**. \*

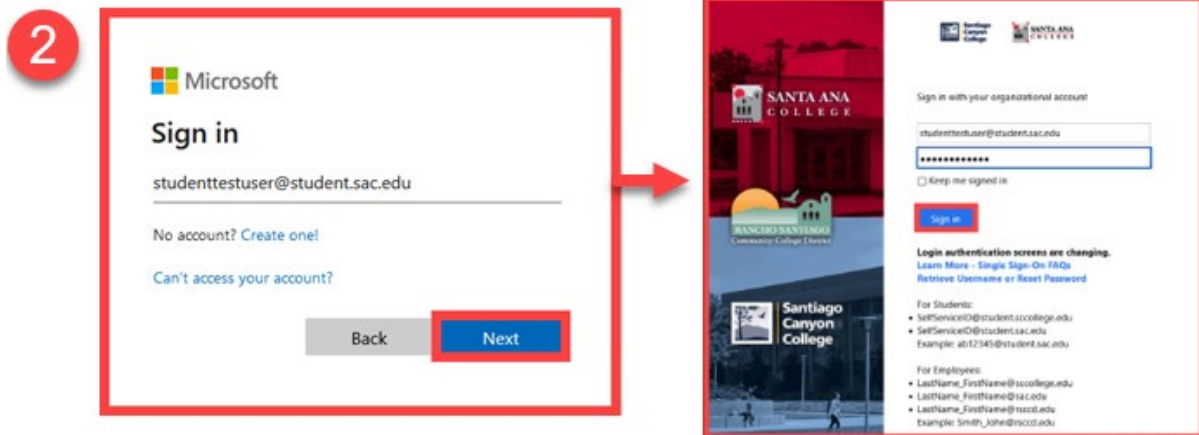
\* **NOTE:** Check that the app is from **Microsoft Corporation**. The app is **free**.



## Step 2 – Sign into your Microsoft account

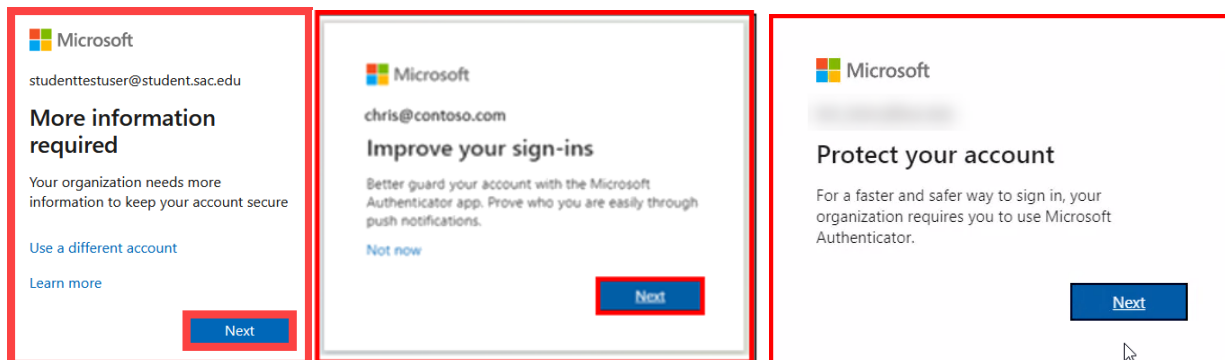
Go to [www.office.com](http://www.office.com) or Outlook Web Access at <https://outlook.office.com>. Sign into your account using your **Single Sign-On credentials**.

We recommend using a **desktop, laptop, or tablet**. Use Google Chrome or Microsoft Edge web browser for the best experience.



## Step 3 - A prompt appears for “More Information required,” “Improve your sign-ins,” or “Protect your account.”

Select **Next**. \*



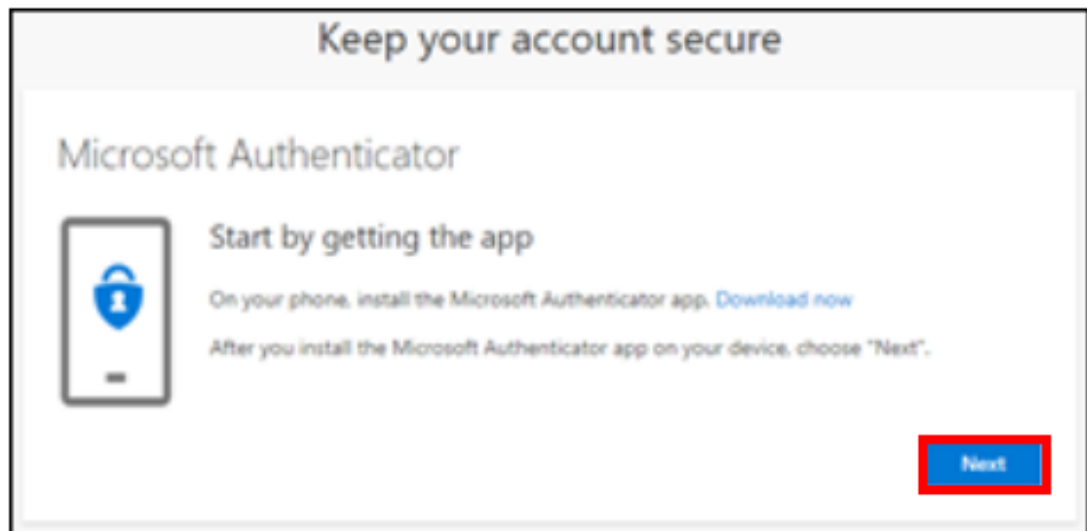
\* **NOTE:** You can select “Not now” to skip the “**Improve your sign-ins**” prompt up to 3 times, but after that, you will be forced to set up Microsoft Authenticator.

Step 4 - At “Keep your account secure” screen, make sure you have the Microsoft Authenticator app already installed on your phone.

If you don't already have the Microsoft Authenticator app, **download it now** following the instructions from [Step 1 – Download the Microsoft Authenticator app](#).

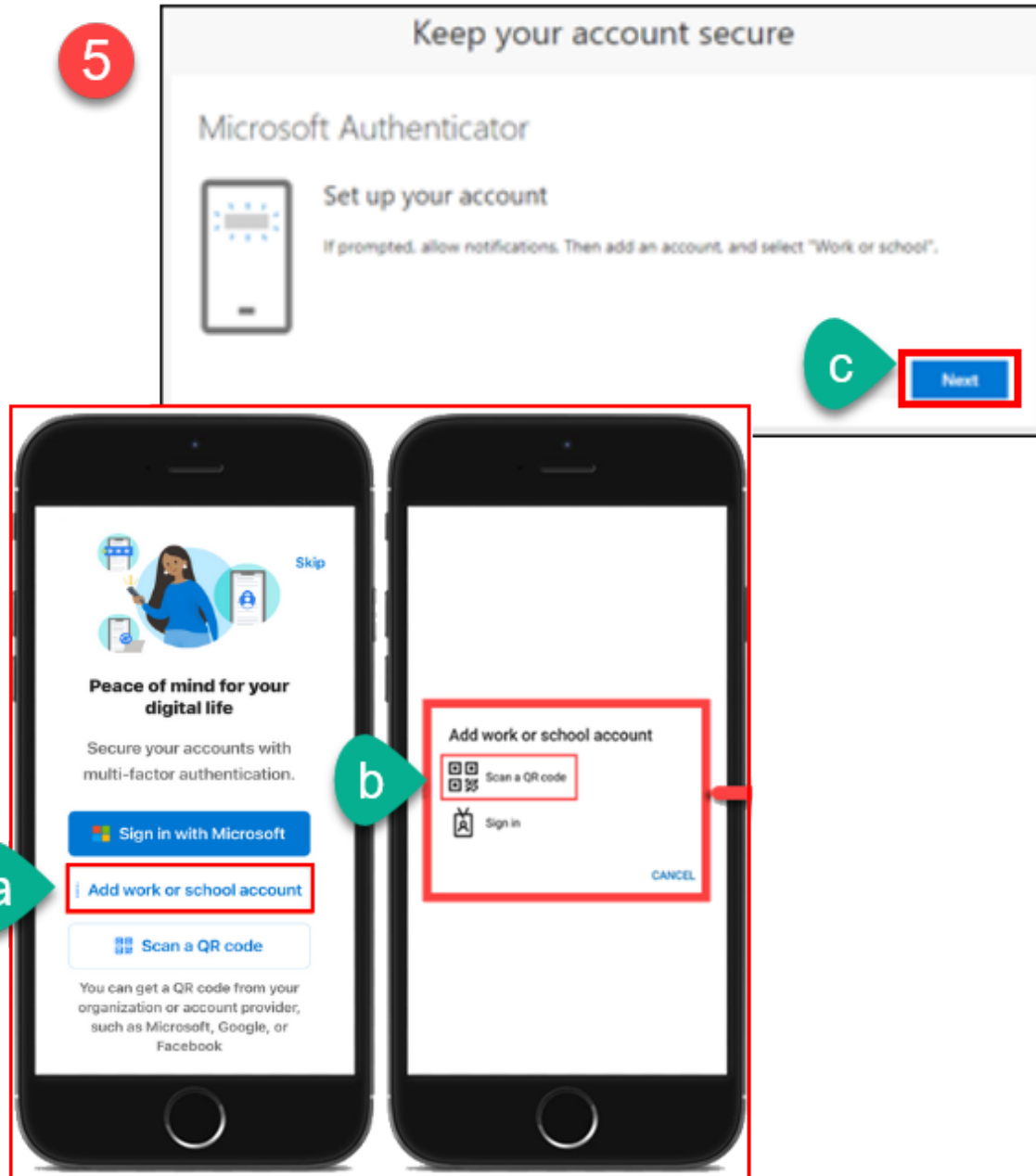
Once you have the app downloaded on your phone, select **Next**.

4



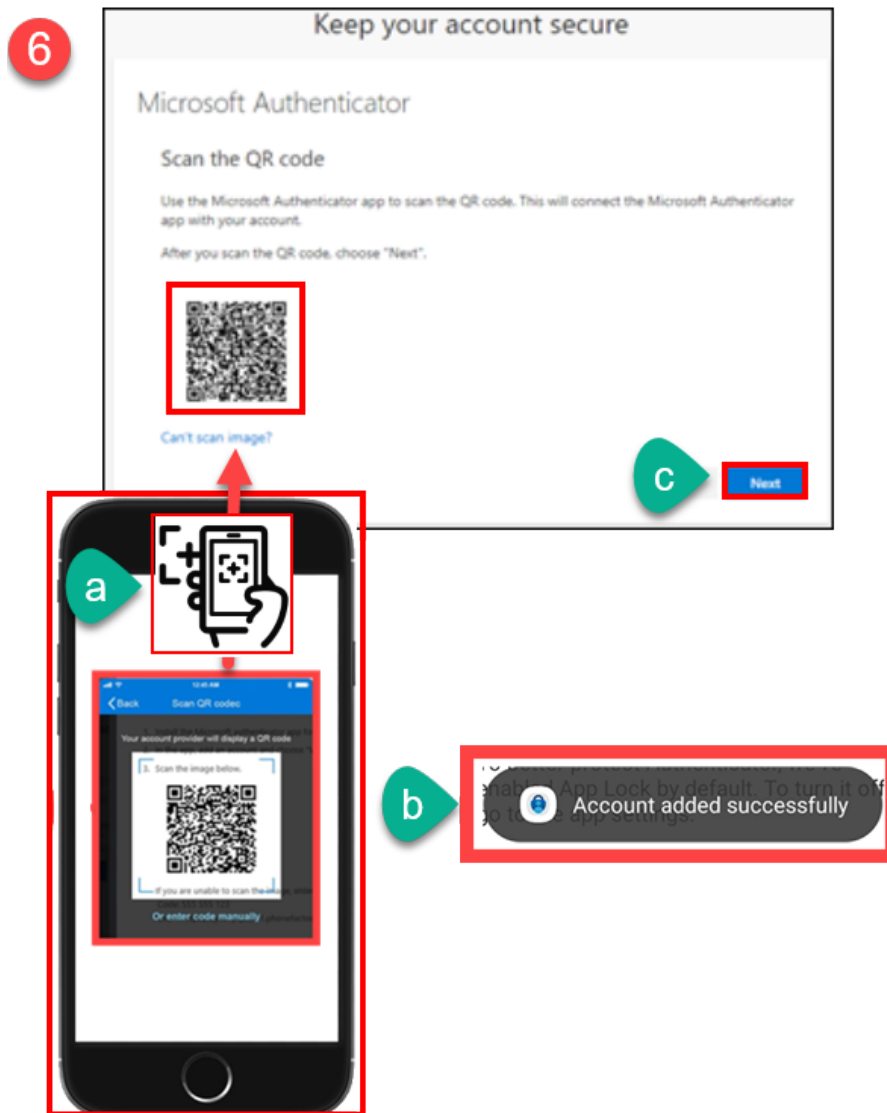
## Step 5 - Follow the prompts to “Set up your account.”

- a. On your phone, open the Microsoft Authenticator app. Tap “Add work or school account.”
  - i. If prompted, allow notifications.
- b. Select “Scan a QR Code”
- c. Select **Next**.



## Step 6 - Scan the QR code displayed on the Microsoft website.

- a. Point your phone's camera at the QR code on screen. \*
- b. The Microsoft Authenticator app will show **"Account added successfully."** The account name shows **Rancho Santiago Community College District** \*\*
- c. Select **Next**.



\* **NOTE:** Scan the QR Code shown on the Microsoft website, not this guide.

\*\* **NOTE:** If Step 5b fails, select "Can't scan image" on the Microsoft webpage, or "enter code manually" from the Microsoft Authenticator app, then following the prompts. You may also contact [ITS Help Desk](#) for help.

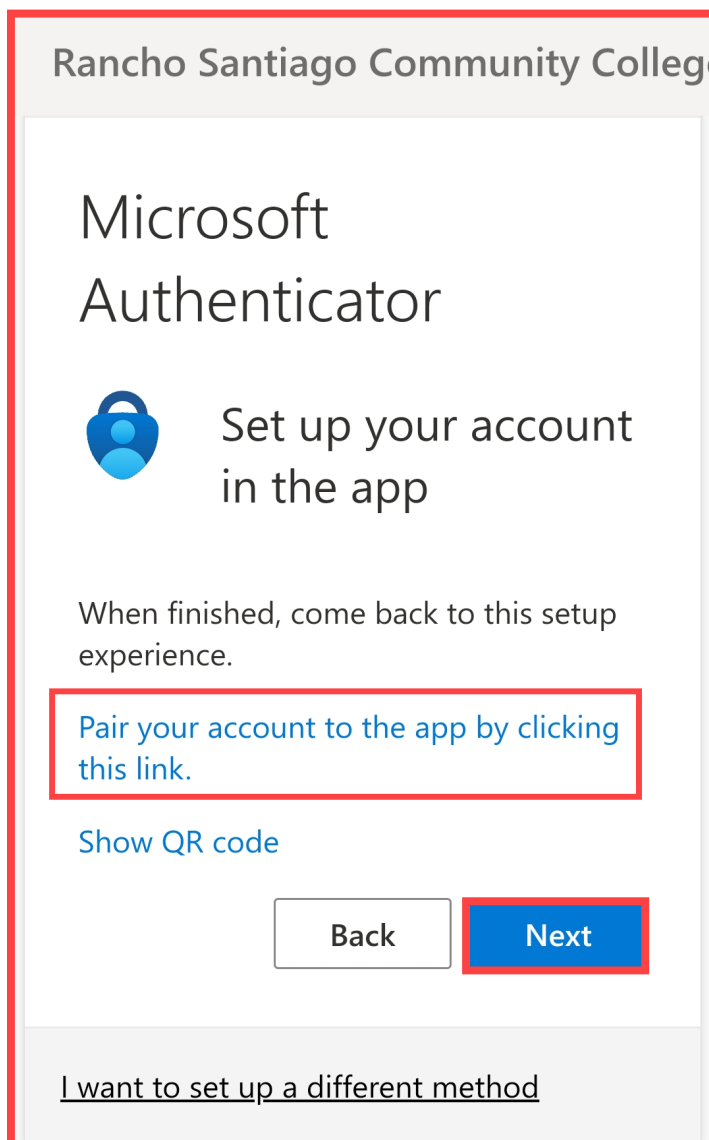
If you initiated MFA setup from your phone instead of a computer:

You'll be prompted with a screen to **"Pair your account to the app by clicking this link"** instead of the QR code.

**If you see this, click the link to pair the app, then click Next.**

Please make sure you installed Microsoft Authenticator app or this won't work.

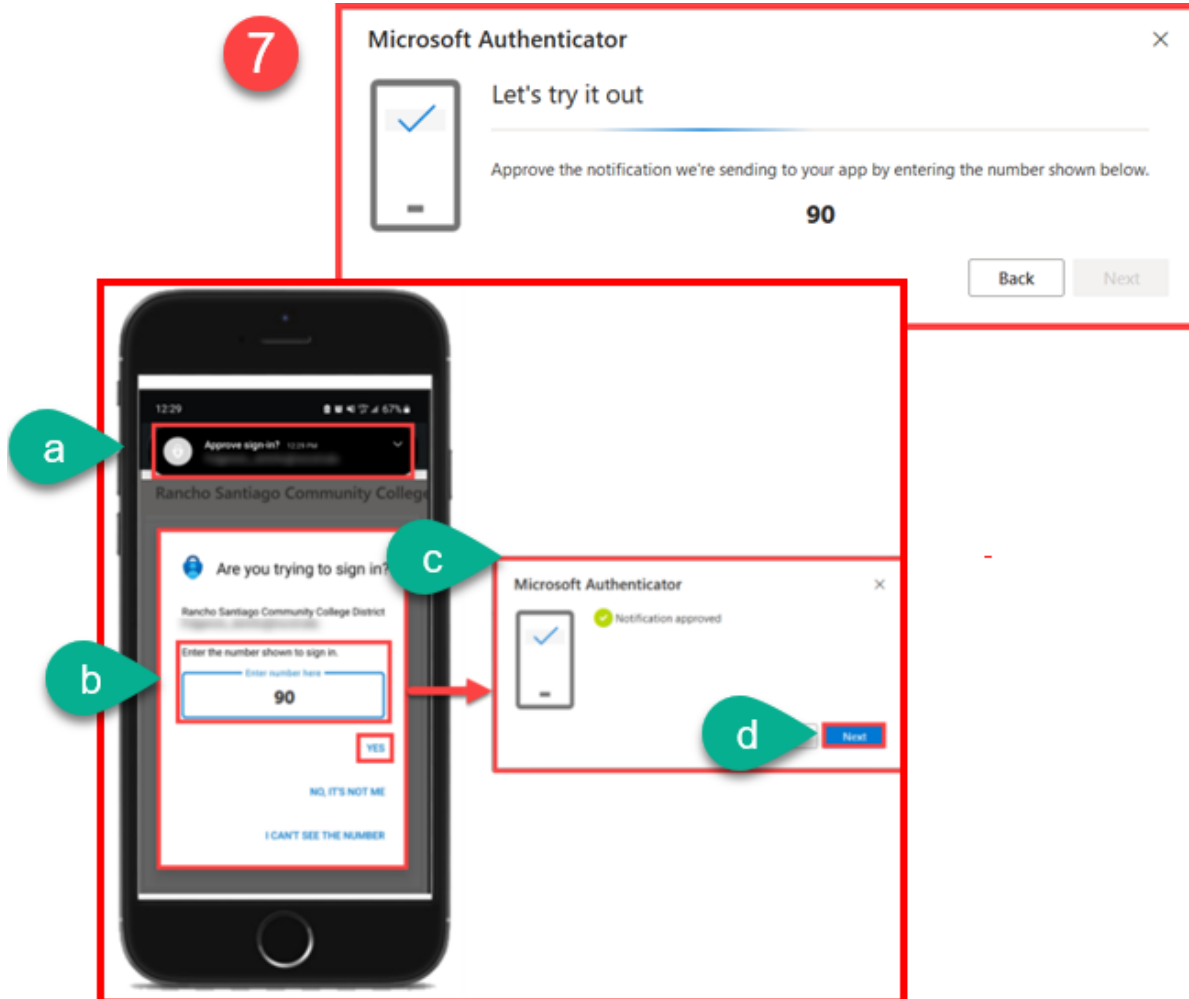
If you don't already have the Microsoft Authenticator app, **download it now** following the instructions from [Step 1 – Download the Microsoft Authenticator app](#).



## Step 7 – Follow the “Let’s try it out” prompts.

### On your phone:

- Select the **Push Notification** asking you to “**Approve sign-in?**”
- Enter the two-digit number** shown and select “**Yes.**” \*
- After approving the sign-in, it will show **Notification approved.** \*\*
- Select **Next** on the notification approved screen to continue.



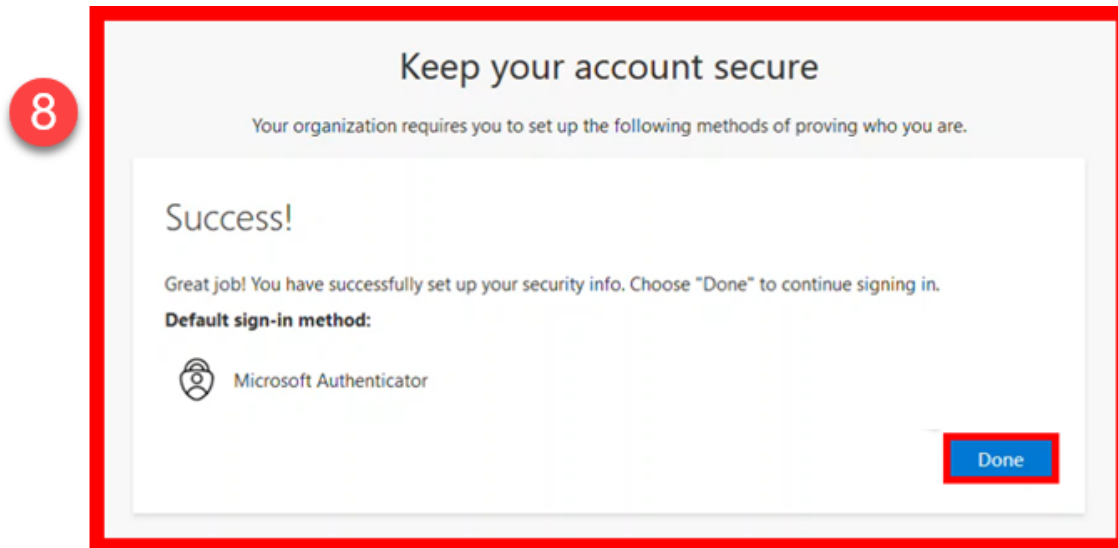
\* **NOTE:** Enter the number shown from the Microsoft site, not this guide.

\*\* **NOTE:** If you can't see the numbers, select “I can't see the number” option from the Microsoft Authenticator prompt app. You may also contact [ITS Help Desk](#) for help.

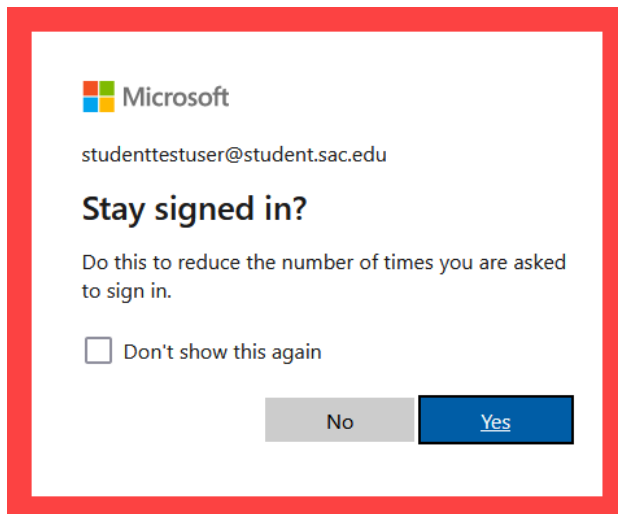
## Step 8 – Complete setup and Office.com login

The next screen prompts “*Success! Great job! You have successfully set up your security info. Choose ‘Done’ to continue signing in. Default sign-in method: Microsoft Authenticator.*”

Select **Done** to finish the set up.



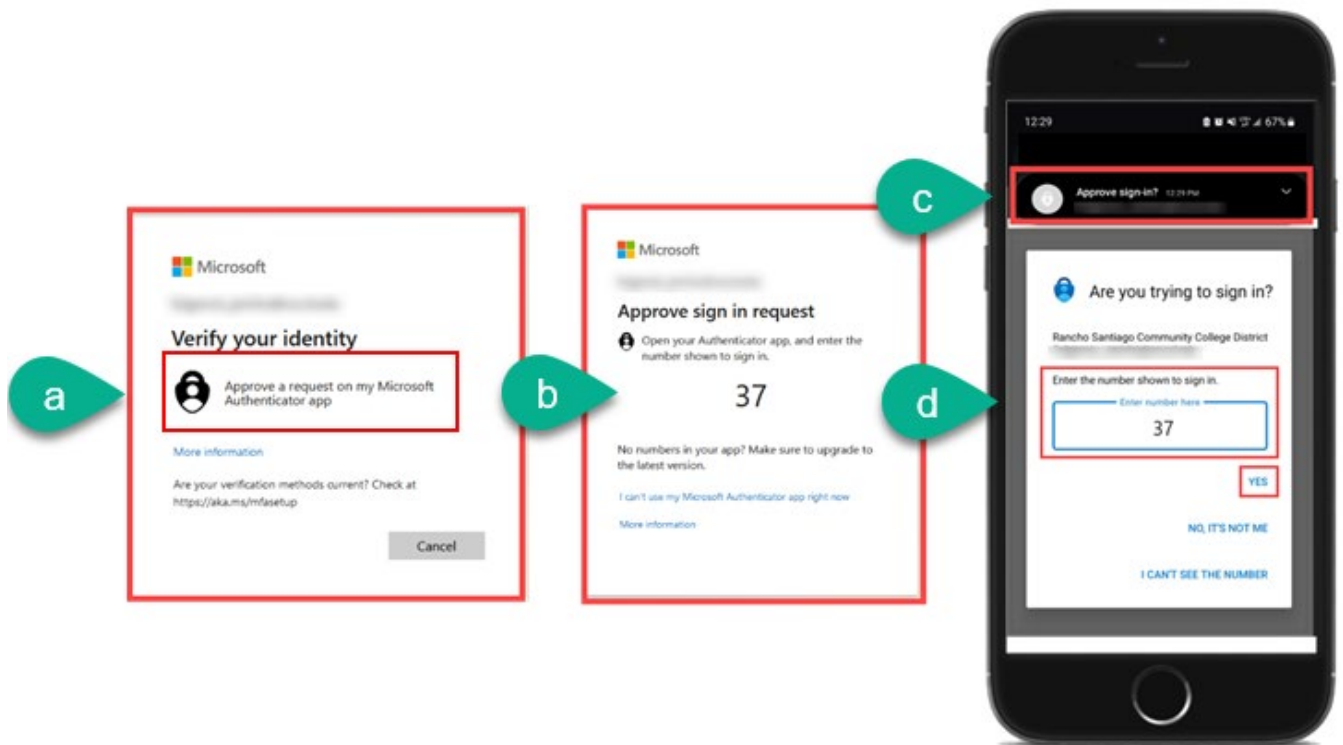
If prompted, select **Yes** or **No** for whether to **Stay signed in** with your account.



## Step 9 - Verify your identity with Microsoft Authenticator on next login

The next time you login and are prompted to **Verify your Identity**:

- a. Select **“Approve a request on my Microsoft Authenticator app.”**
- b. A two-digit code will appear on the screen.
- c. On your phone, select the push notification to **“Approve sign-in?”**, or **open the Microsoft Authenticator app** yourself. \*
- d. **Enter the number shown on the screen, then select “Yes.”** \*\*



\* **NOTE:** If your mobile phone locks with a PIN, password, fingerprint, facial recognition, etc., you may need to verify with that to Approve sign-in.

\*\* **NOTE:** Only **“Approve”** Microsoft Authenticator prompts that you initiate yourself. If you receive an unknown prompt, you did not initiate, select **“No, it’s not me”** on the prompt and contact the [ITS Help Desk](#).



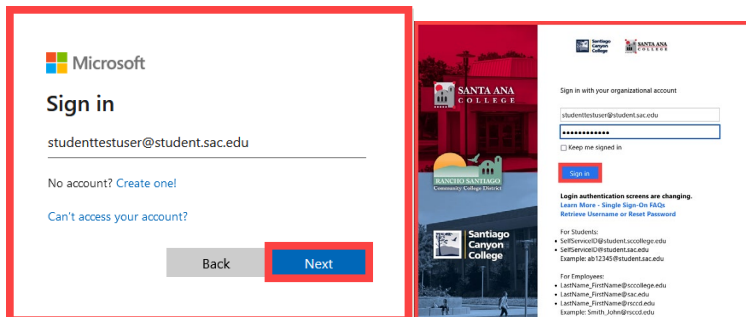
# Google Authenticator

**NOTE:** This requires a mobile device with access to the Google Authenticator app.

## Step 1 – Login to Microsoft website

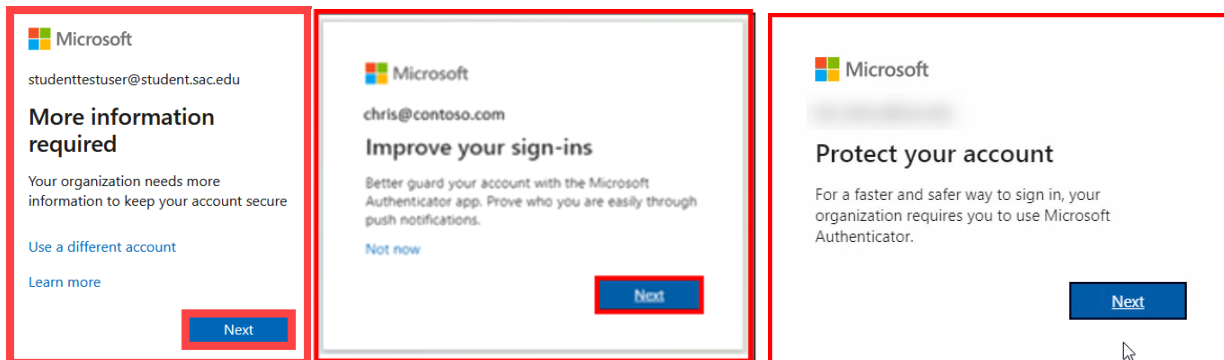
Go to [www.office.com](https://www.office.com) or Outlook Web Access at <https://outlook.office.com>.  
Sign into your account using your **Single Sign-On credentials**.

We recommend using a **desktop, laptop, or tablet**. Use Google Chrome or Microsoft Edge web browser for the best experience.



## Step 2 - A prompt appears for “More Information required,” “Improve your sign-ins,” or “Protect your account.”

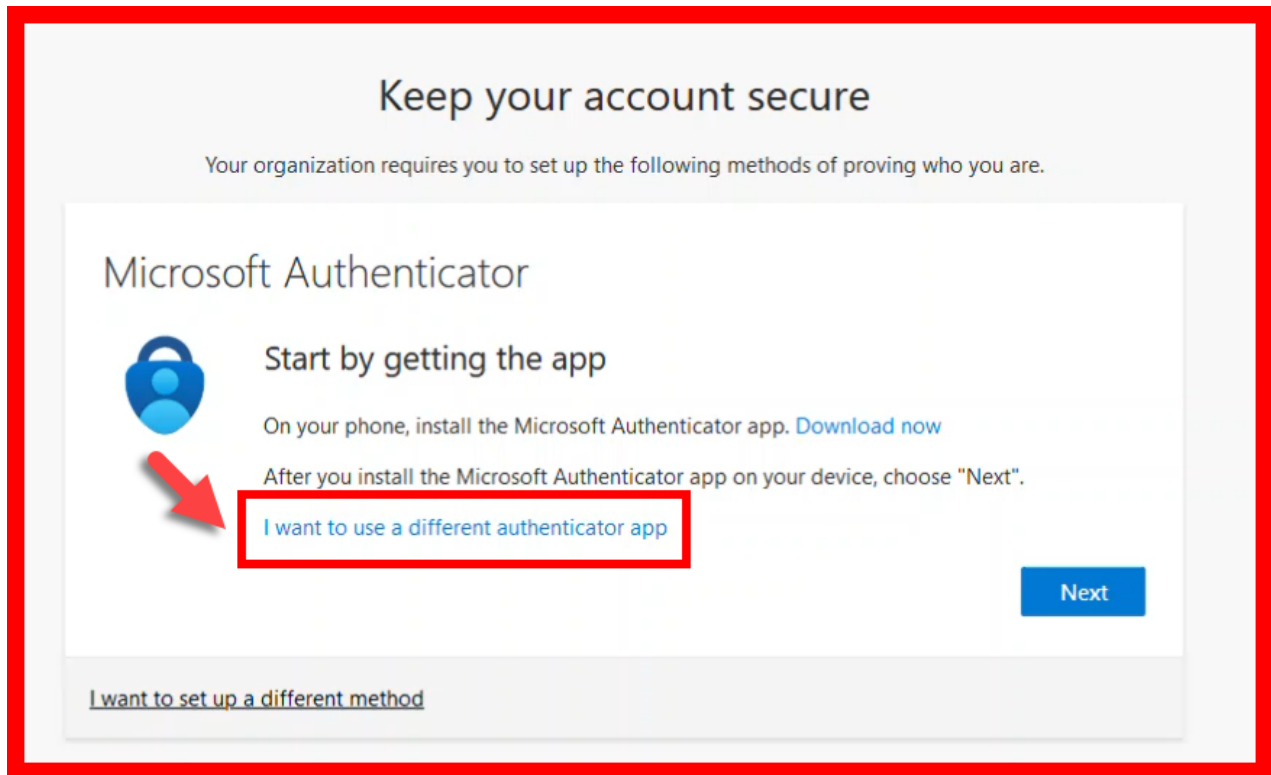
Select **Next**. \*



\* **NOTE:** You can select “Not now” to skip the “**Improve your sign-ins**” prompt up to 3 times, but after that, you will be forced to set up Microsoft Authenticator.

### Step 3 – Select “I want to set up a different authenticator app.”


Select **I want to use a different authenticator app.**



Keep your account secure

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

#### Microsoft Authenticator



**Start by getting the app**

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose "Next".

[I want to use a different authenticator app](#)

[Next](#)

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

## Step 4 – Download and install the Google Authenticator app

On your phone, **download and install** the **Google Authenticator** app.

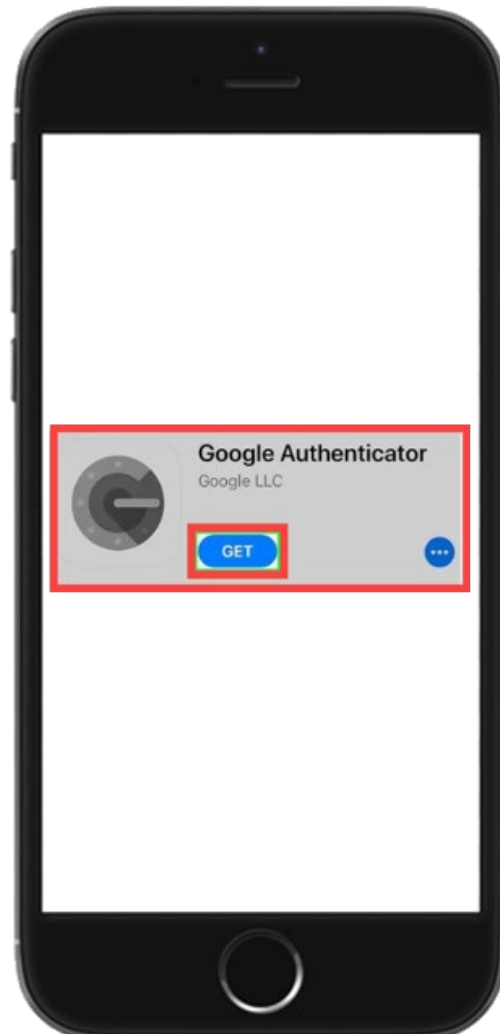
**NOTE:** *The official version is from **Google LLC**.*

Once you have downloaded and installed Google Authenticator, continue with the set up prompts from the Microsoft website.

[Google Play store \(Android\):](#)



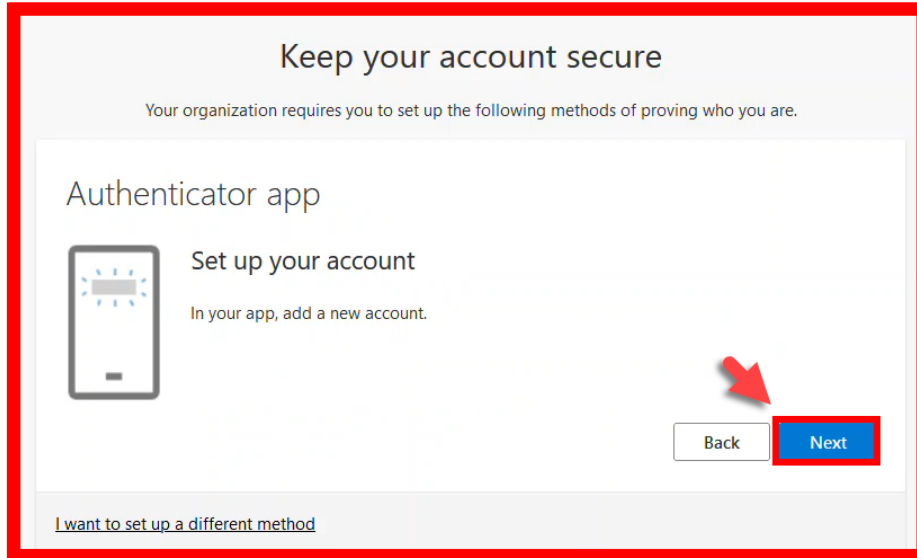
[App Store \(iOS\):](#)



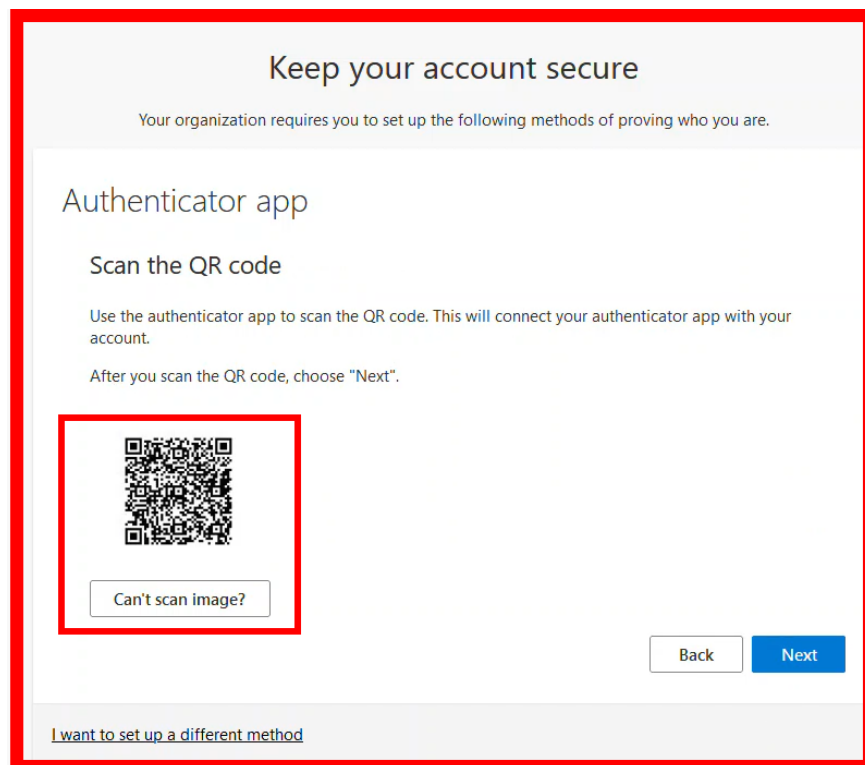
## Step 5 – Set up your account and scan the QR code

On the **Set up your account** screen, it instructs *“In your app, add a new account.”*

Select **Next** to continue.

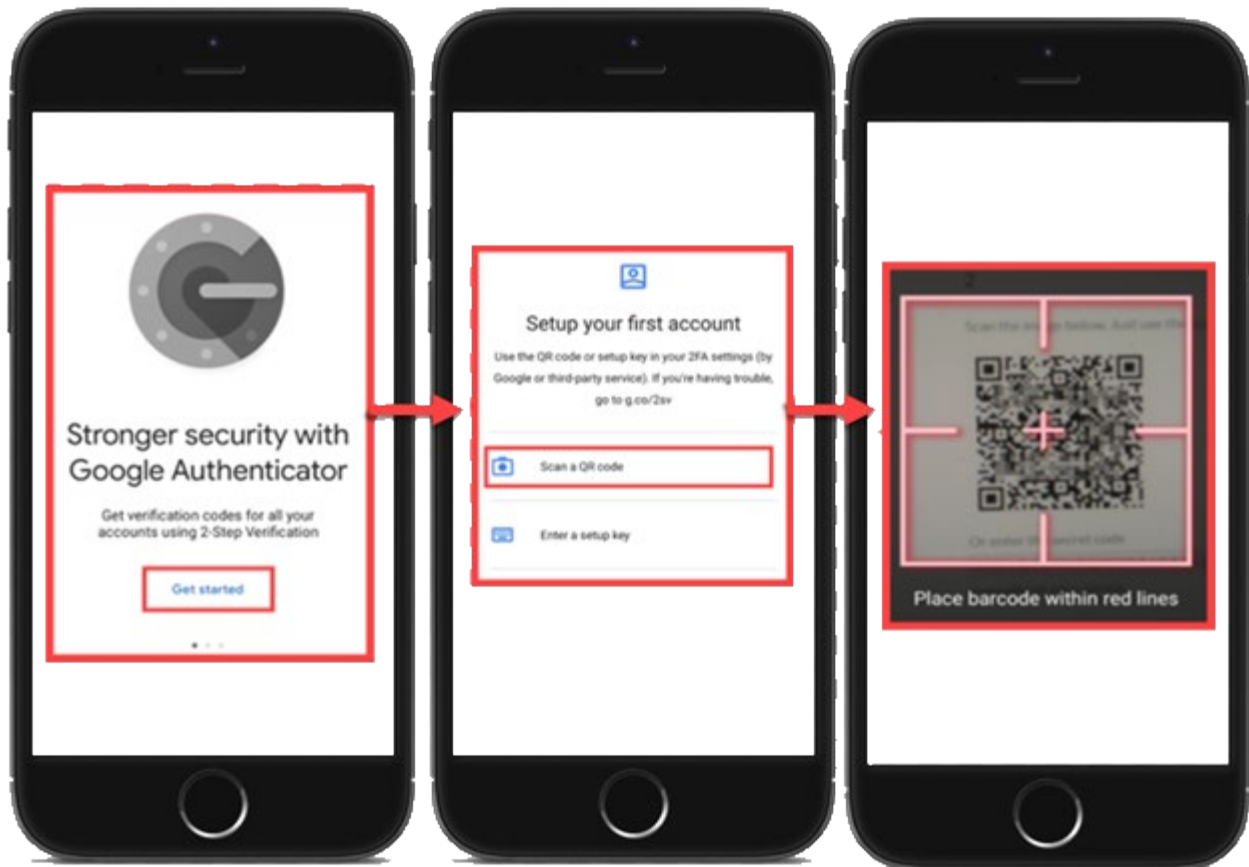


The **Scan the QR code** screen instructs: *“Use the authenticator app to scan the QR code. This will connect your authenticator app with your account.”*



On your mobile device, open Google Authenticator app.

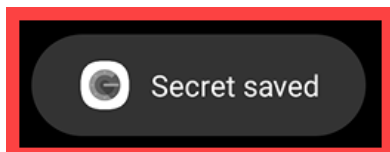
1. Select **Get Started** to **Setup your first account**.
2. Select **Scan a QR code**. (Or select add “+” and then Scan a QR code.)
3. **Point your mobile phone’s camera to the QR code on screen so it scans.**



After scanning the QR code, a confirmation will say *“Account added”*.

The account name shows as: Microsoft (**Rancho Santiago Community College District**), followed by the verification code that auto-refreshes.

Select **Add Account** to continue. The app will show the message **“Secret Saved.”**



Return to the **Keep your account secure** screen and select **Next** to continue.

## Keep your account secure


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

### Authenticator app

#### Scan the QR code

Use the authenticator app to scan the QR code. This will connect your authenticator app with your account.

After you scan the QR code, choose "Next".



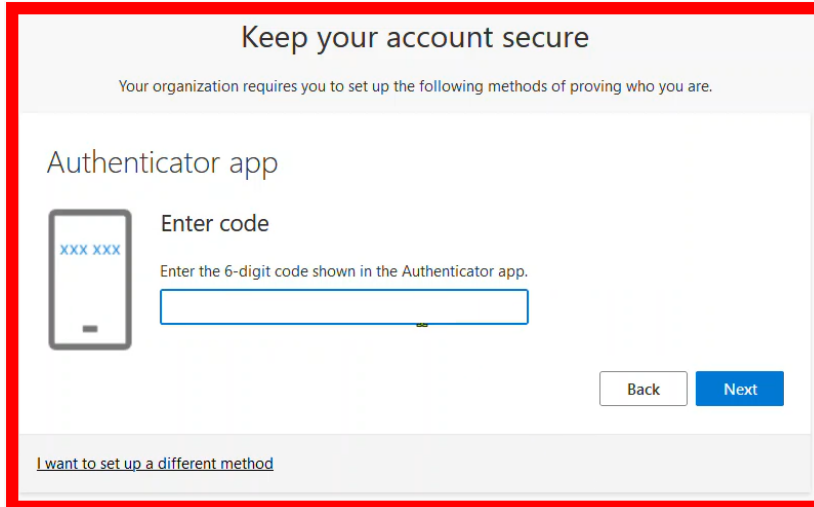
[Can't scan image?](#)

[Back](#) [Next](#)

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

## Step 6 – Verify the Google Authenticator app works

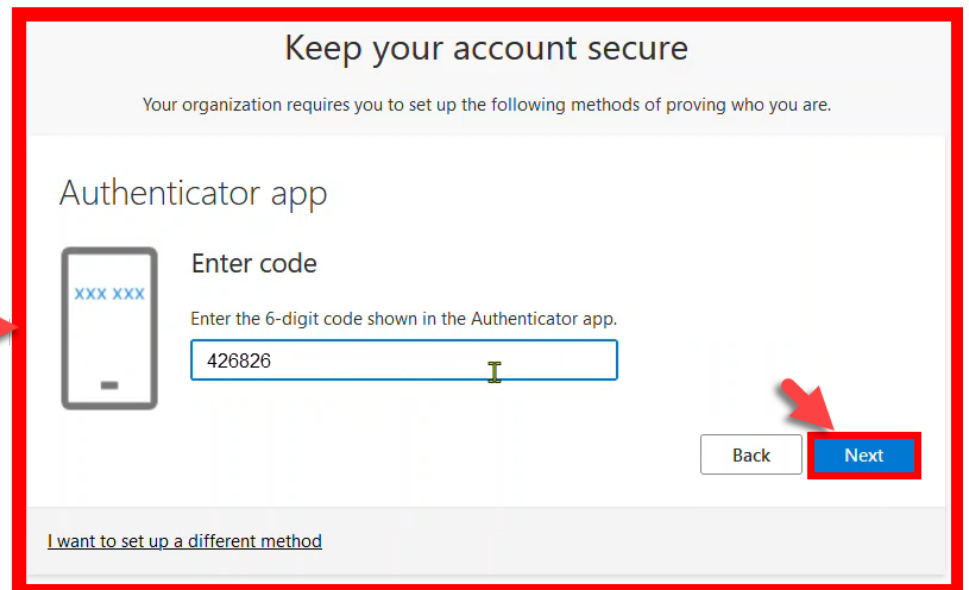
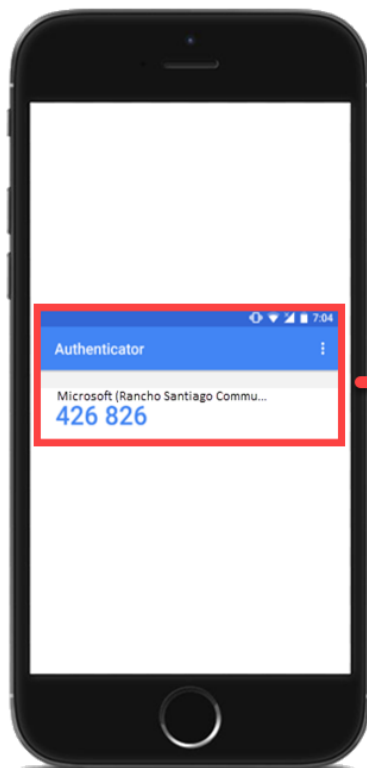
The **Enter code** screen asks, *“Enter the 6-digit code shown in the Authenticator app.”*



The screenshot shows a web page titled "Keep your account secure" with the subtext "Your organization requires you to set up the following methods of proving who you are." Below this, the "Authenticator app" section is highlighted with a red border. It features a placeholder image of a smartphone displaying "xxx xxx". To the right, the text "Enter code" is followed by "Enter the 6-digit code shown in the Authenticator app." and an empty input field. At the bottom right of this section are "Back" and "Next" buttons. A link at the bottom left reads "I want to set up a different method".

**On your phone**, open Google Authenticator app and enter the verification code that appears for **Microsoft (Rancho Santiago Community College District)**.

After you have entered the code, select **Next** to continue.



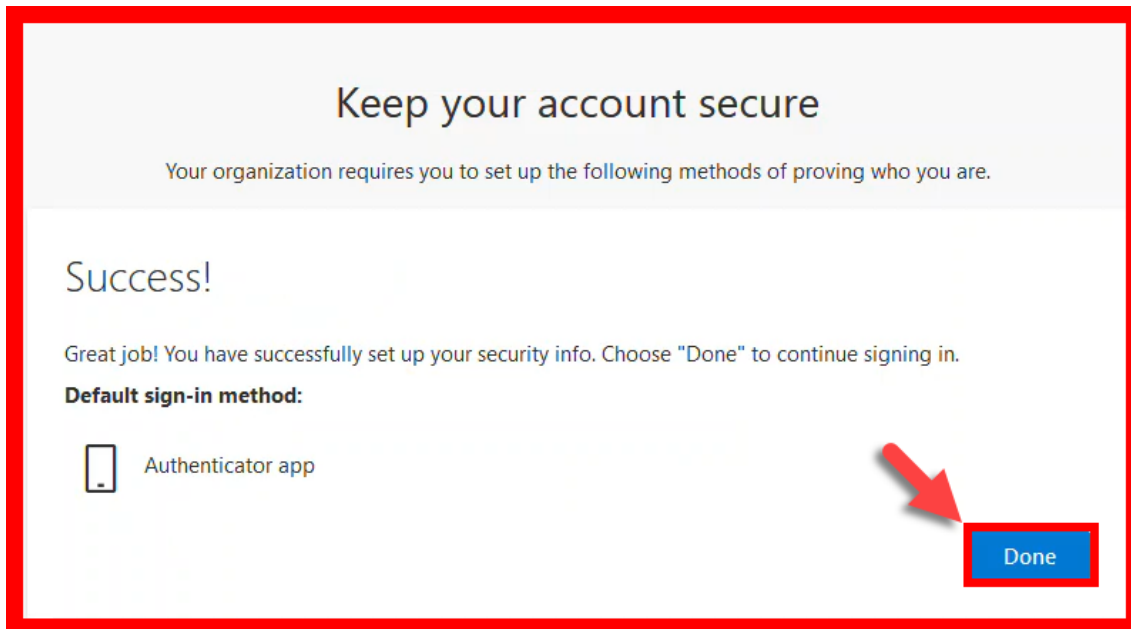
This screenshot is identical to the previous one but shows the verification code "426826" entered into the input field. A red arrow points to the "Next" button, which is also highlighted with a red box. The "Back" button remains unhighlighted.

## Step 7 – Complete setup and Office.com login

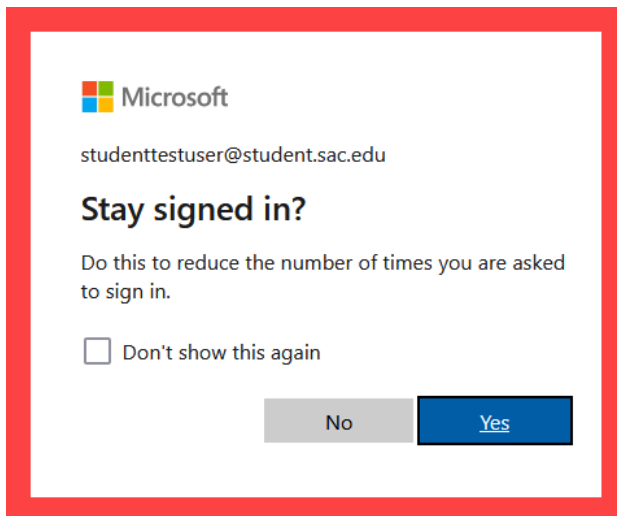
The next screen prompts *Success! Great job! You have successfully set up your security info. Choose "Done" to continue signing in.*

*Default sign-in method: Authenticator app*

Select **Done** to finish the set up.



If prompted, select **Yes** or **No** for whether to **Stay signed in** with your account.

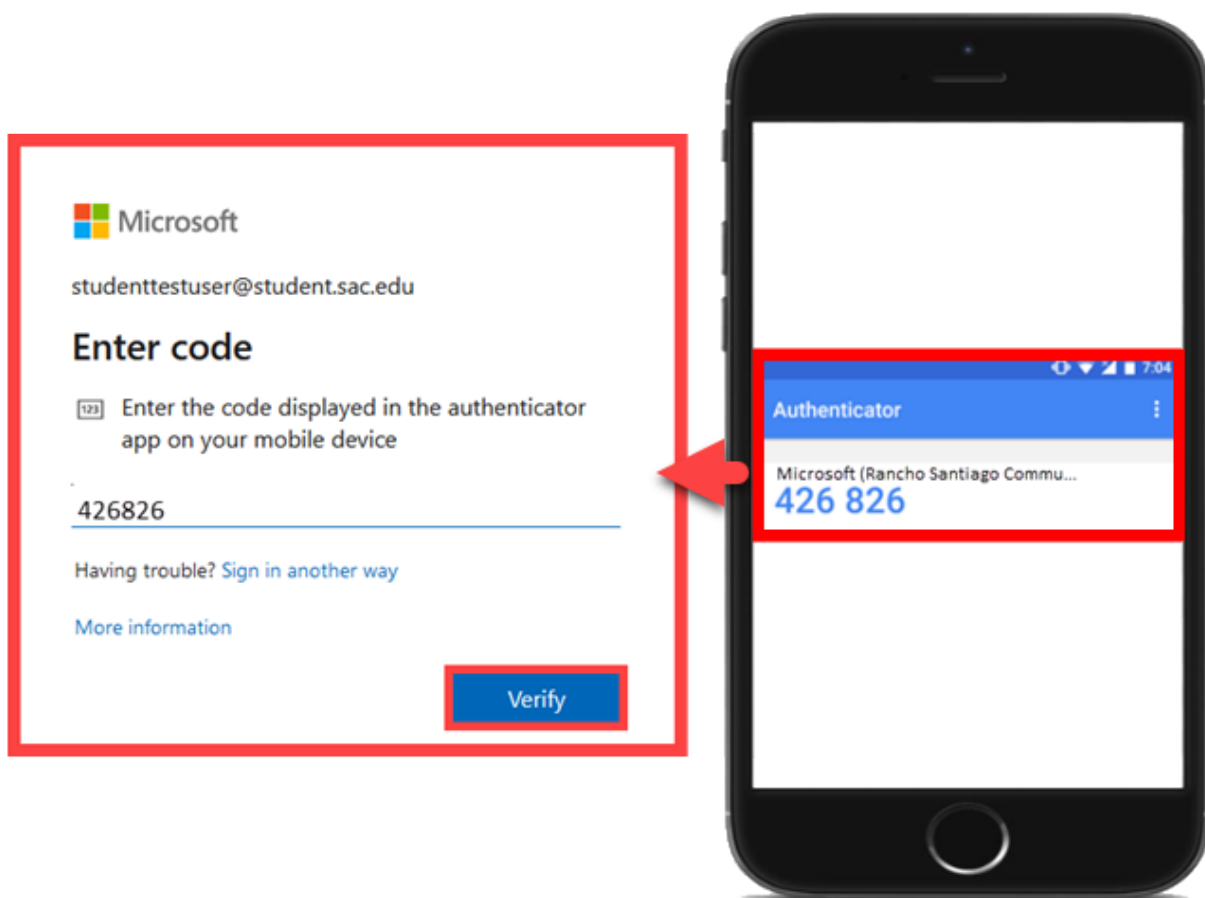


After verification and signing in, you will return to **Office.com home page** for the **Microsoft 365 portal**.

## Step 8 - Verify your identity with Google Authenticator on next login

The next time you login and are prompted to **Verify your Identity**:

1. Follow the prompt to *“Enter the code displayed in the authenticator app on your mobile device”*
2. **On your mobile phone**, open the Google Authenticator app.
3. **Enter the verification code** you see under **Microsoft (Rancho Santiago Community College District)**.
4. Select **Verify** to continue.



**NOTE: Only “Verify”** Google Authenticator verification codes that you initiate yourself. If you receive an unknown prompt, you did not initiate, ignore the prompt, and contact the [ITS Help Desk](#).



## Phone Call

**NOTE:** This requires an office phone or phone number that can receive voice calls.

### Step 1 – Login to Microsoft website

Go to [www.office.com](http://www.office.com) or Outlook Web Access at <https://outlook.office.com>. Sign into your account using your **Single Sign-On credentials**.

We recommend using a **desktop, laptop, or tablet**. Use Google Chrome or Microsoft Edge web browser for the best experience.

Microsoft  
Sign in  
studenttestuser@student.sac.edu  
No account? [Create one!](#)  
[Can't access your account?](#)

Back **Next**

Sign in with your organizational account  
studenttestuser@student.sac.edu  
\*\*\*\*\*  
 Keep me signed in  
**Sign in**

Login authentication screens are changing.  
[Learn More - Single Sign-On FAQs](#)  
[Retrieve Username or Reset Password](#)

For Students:  
• SelfServiceID@student.sacollege.edu  
• SelfServiceID@student.sac.edu  
• Example: ab12345@student.sac.edu

For Employees:  
• LastName\_FirstName@scollege.edu  
• LastName\_FirstName@sac.edu  
• LastName\_FirstName@rscsd.edu  
• Example: Smith\_John@rscsd.edu

### Step 2 - A prompt appears for “More Information required,” “Improve your sign-ins,” or “Protect your account.”

Select **Next**. \*

Microsoft  
studenttestuser@student.sac.edu  
**More information required**  
Your organization needs more information to keep your account secure  
[Use a different account](#)  
[Learn more](#)  
**Next**

Microsoft  
chris@contoso.com  
**Improve your sign-ins**  
Better guard your account with the Microsoft Authenticator app. Prove who you are easily through push notifications.  
[Not now](#)  
**Next**

Microsoft  
**Protect your account**  
For a faster and safer way to sign in, your organization requires you to use Microsoft Authenticator.  
**Next**

\* **NOTE:** You can select “Not now” to skip the “**Improve your sign-ins**” prompt up to 3 times, but after that, you will be forced to set up Microsoft Authenticator.

### Step 3 – Select “I want to set up a different method”, then select Phone.

Select **I want to set up a different method**. Select **Phone**.

Keep your account secure

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

Microsoft Authenticator

Start by getting the app

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose "Next".

[I want to use a different authenticator app](#)

Next

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

Choose a different method

Which method would you like to use?

Phone

Cancel Confirm

### Step 4 – Enter phone number, then select “Call Me”

Enter your **phone number** and select **Call me**. Select **Next** to continue.

Keep your account secure

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

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?

United States (+1) 714

Text me a code

Call me

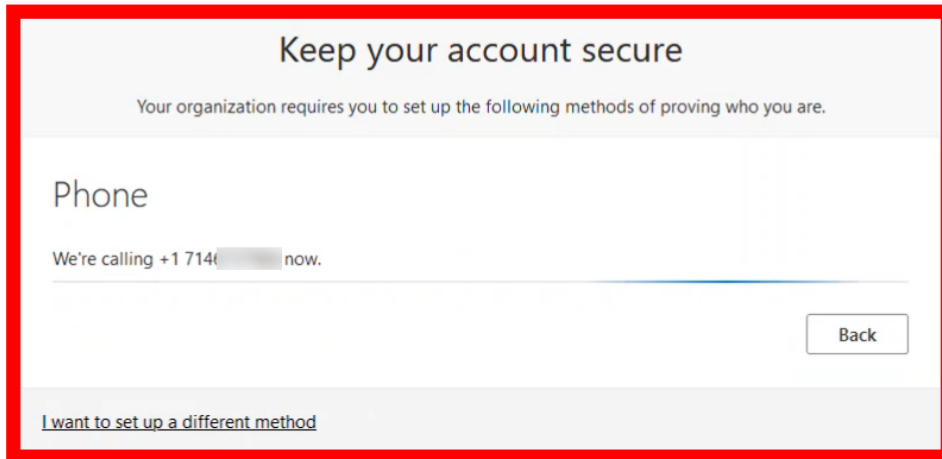
Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).

Next

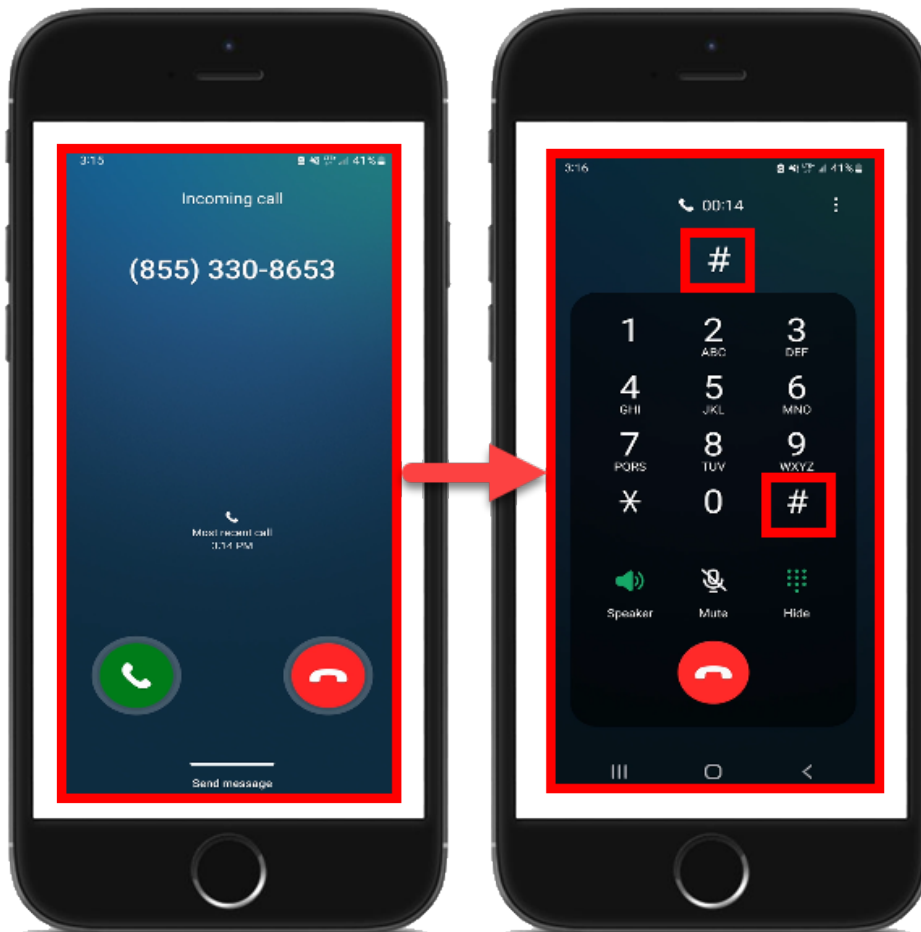
[I want to set up a different method](#)

**Step 5 – Answer the phone call from Microsoft and press # key to verify.**

The next screen instructs, *“We’re calling your phone number now.”*

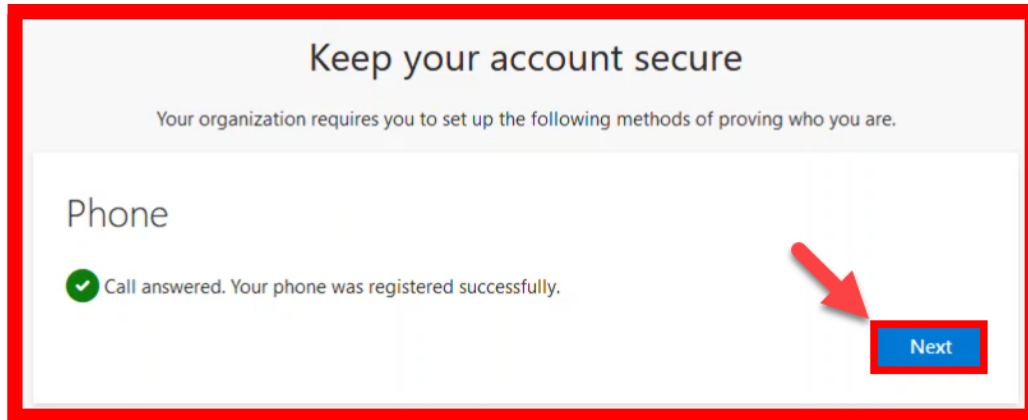


**On your phone, answer the call from Microsoft.** Follow the prompts from the call, and **select the # key** to verify the sign in.



## Step 6 – Complete setup and Office.com login

Select **Next** to continue.



Keep your account secure

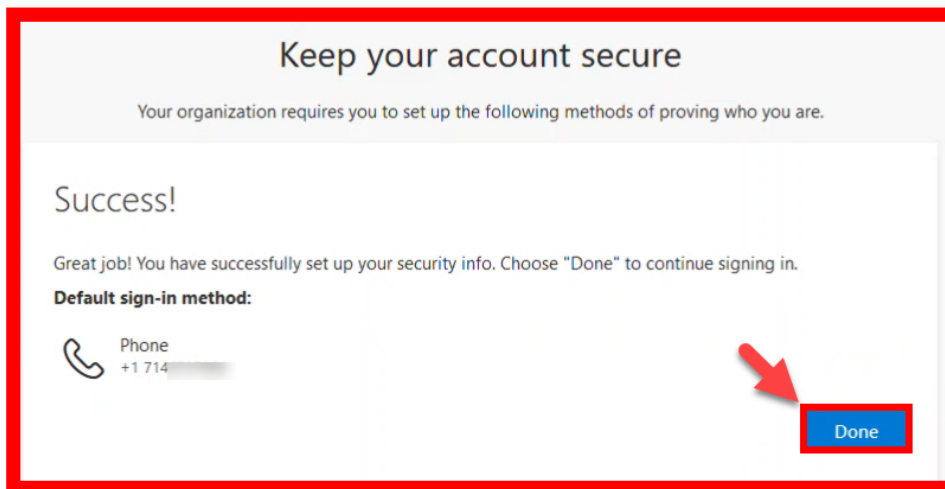
Your organization requires you to set up the following methods of proving who you are.

Phone

✓ Call answered. Your phone was registered successfully.

Next

Select **Done** to finish the set up.



Keep your account secure

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

Success!

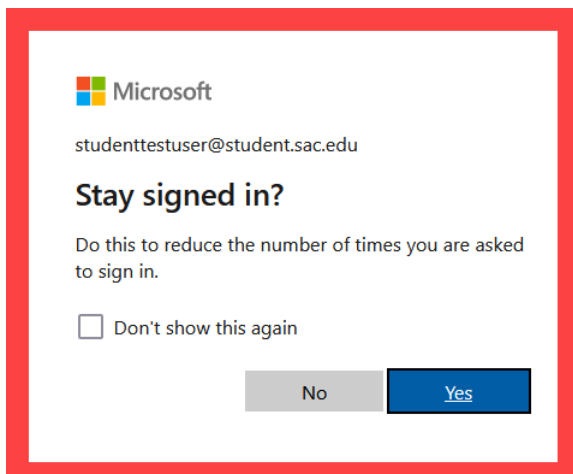
Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

**Default sign-in method:**

Phone +1 714

Done

If prompted, select **Yes** or **No** for whether to **Stay signed in** with your account.



Microsoft

studenttestuser@student.sac.edu

**Stay signed in?**

Do this to reduce the number of times you are asked to sign in.

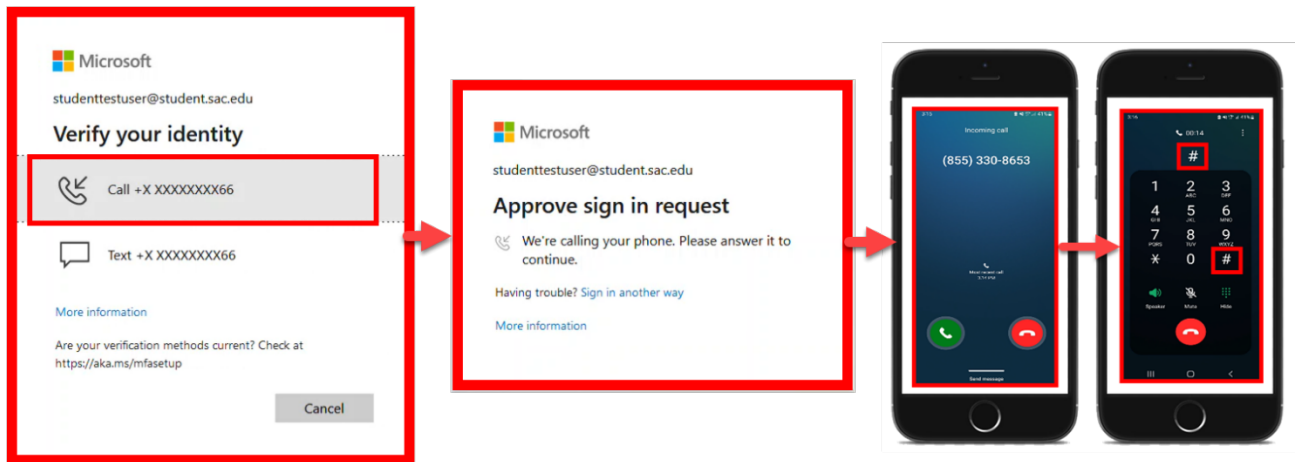
Don't show this again

No Yes

## Step 7 – Verify your identity with Phone call on next login

The next time you login to and are prompted to **Verify your Identity**:

1. Select the **Call +X XXXXXXXX** option.
2. The **Approve sign in request** prompt instructs, *“We’re calling your phone. Please answer it to continue.”*
3. **Answer the phone call from Microsoft.**
4. **Press the # key** to authenticate the sign-in.



**NOTE: Only “verify” or authenticate phone calls from Microsoft that you have initiated yourself.**

If you receive an unknown text prompting you to input a verification code that you did not initiate, ignore the prompt, and contact the [ITS Help Desk](#).



## Hardware Token

**NOTE:** This requires a physical Hardware Token provided by the ITS Department.

### Step 1 – Request a Hardware Token from the ITS Department

Contact the [ITS Help Desk](#) to request a physical Hardware Token.

When submitting your request, please specify your **Name, District Email Address, Employee ID Number, and Preferred Pickup Location.**

Once your request has been approved, a device will be issued for you, and a technician will be coordinate a day/time to provide you the device at your Preferred Pickup Location.



Proceed to [Office.com login](#) once ITS has issued your Hardware Token device.

### Step 2 – Login to Office.com with your Single Sign-On (SSO) username

[Login to Office.com website with your Single Sign-On \(SSO\) username.](#)

### Step 3 – Enter the Verification Code

When prompted to **Enter code:**

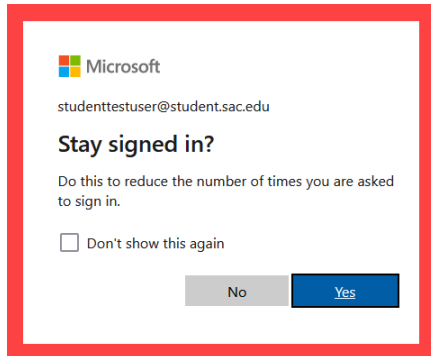
1. Press the **Power Button** to **turn on the Hardware Token.**
2. Enter the **6-digit authentication code** that appears on the Hardware Token.
3. Select **Verify** to continue.

**NOTE:** The Hardware Token code refreshes every **30 seconds.**



## Step 4 – Complete Office.com login

If prompted, select **Yes** or **No** for whether to **Stay signed in** with your account.

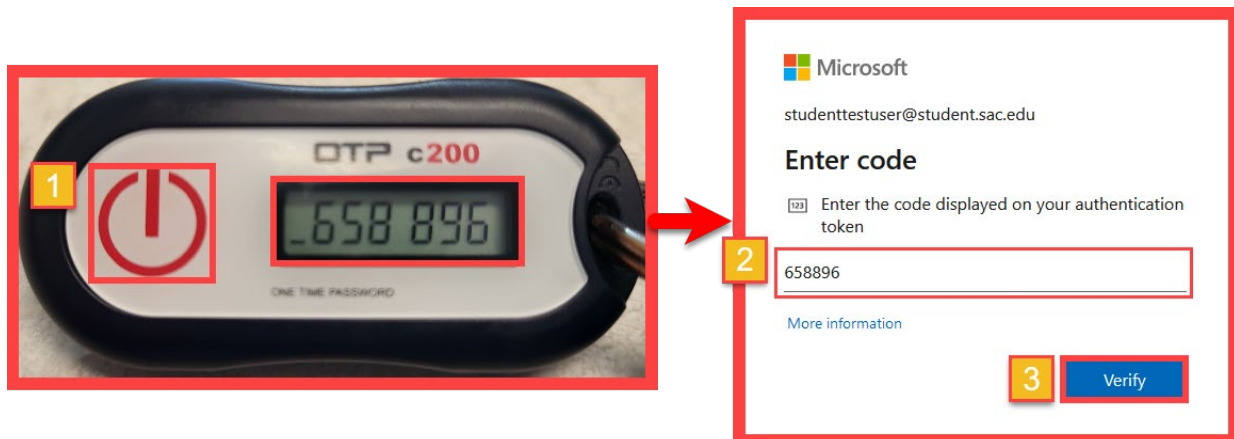


## Step 5 - Verify your identity with Hardware Token on next login

The next time you login to and are prompted to **Verify your Identity**:

1. Press the **Power Button** to **turn on the Hardware Token**.
2. Enter the **6-digit authentication code** that appears on the Hardware Token.
3. Select **Verify** to continue.

**NOTE:** The Hardware Token code refreshes every **30 seconds**.



**NOTE:** ITS recommends keeping the Hardware Token on your person at all times, or locked in a secure place when not in use.

If the Hardware Token is lost or stolen, it will not to be deactivated by an admin. Contact the [ITS Help desk](#) for help with this.

If a bad actor gains physical access to your Hardware Token they can use it to authenticate your login, although they would also need to know your password.

# Manage your backup authentication methods

Follow these steps to set up a **backup authentication method** or to **manage your existing MFA method(s)**.

## Step 1 – Sign into <https://aka.ms/mfasetup>

From your computer, go to the website <https://aka.ms/mfasetup> and **Sign In**. Enter your **Single sign-on (SSO) username** and select **Next**.

Microsoft  
Sign in  
studenttestuser@student.sac.edu  
No account? [Create one!](#)  
Can't access your account?  
Back Next

Santa Ana College  
RANCHO SANTIAGO  
Community College District  
Santiago Canyon College

Sign in with your organizational account  
studenttestuser@student.sac.edu  
\*\*\*\*\*  
 Keep me signed in  
Sign in

Login authentication screens are changing.  
[Learn More - Single Sign-On FAQs](#)  
[Retrieve Username or Reset Password](#)

For Students:  
• SelfServiceID@student.sccollege.edu  
• SelfServiceID@student.sac.edu  
Example: ab12345@student.sac.edu

For Employees:  
• LastName\_FirstName@sccollege.edu  
• LastName\_FirstName@sac.edu  
• LastName\_FirstName@rscsd.edu  
Example: Smith\_John@rscsd.edu

When prompted, verify your identity. \*

Microsoft  
studenttestuser@student.sac.edu  
Verify your identity

Approve a request on my Microsoft Authenticator app

Use a verification code

Text +X XXXXXXXXX66

Call +X XXXXXXXXX66

[More information](#)

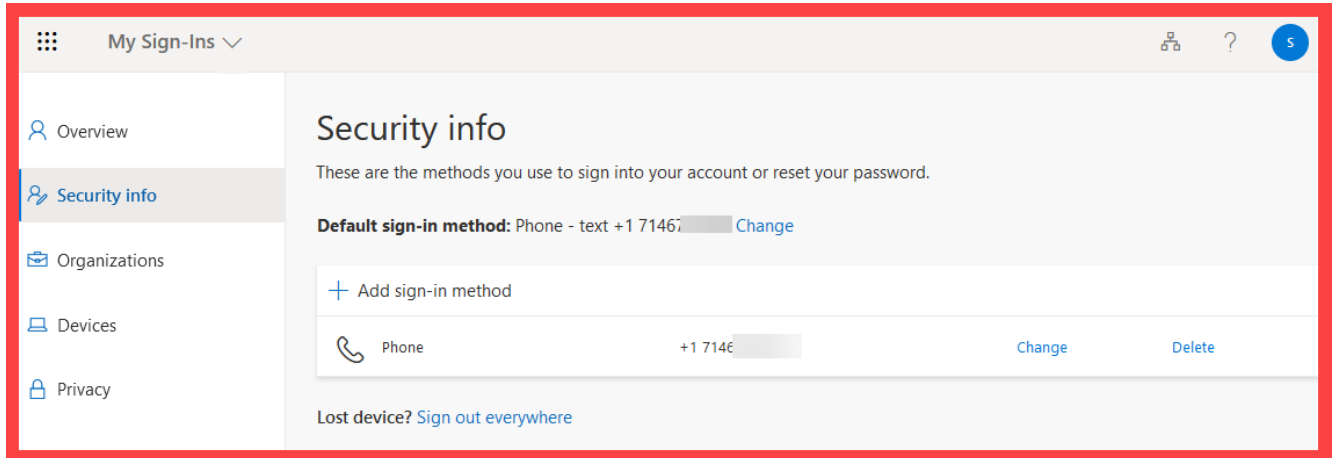
Are your verification methods current? Check at <https://aka.ms/mfasetup>

Cancel

**\* NOTE:** If you don't already have MFA, you'll be prompted to set it up now. Return to the [Table of Contents](#) of this guide for instructions on how to set up your MFA method of choice.

## Step 2 – Add, Delete, or Change your sign-in methods

From the **Security Info** page, you can [change](#), [add](#), or [delete](#) your sign-in methods.

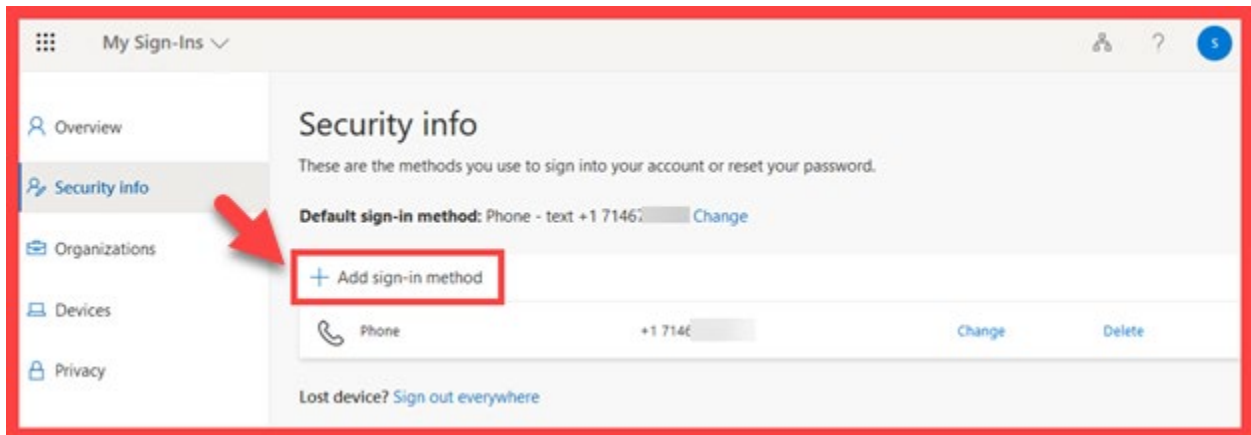


- [Add a sign-in method](#)
- [Delete a sign-in method](#)
- [Change Default sign-in method](#)
- [Change the properties of an existing sign-in method](#)

**ITS strongly recommends setting up a backup authentication method.**

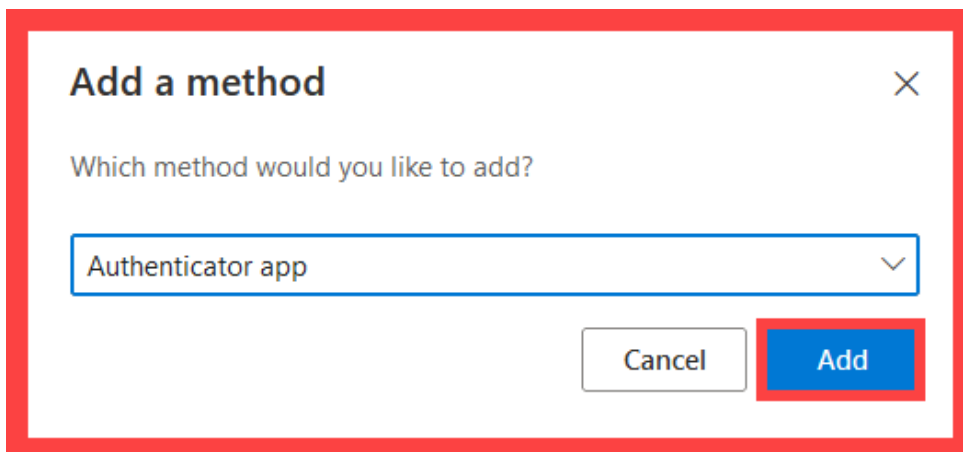
## Step 3a - Add a sign-in method

To add a sign-in method, select **Add sign-in method**.



Select another method to add from the dropdown list, then select **Add**.

*Examples of other methods would be Authenticator app or an Alternate phone.*



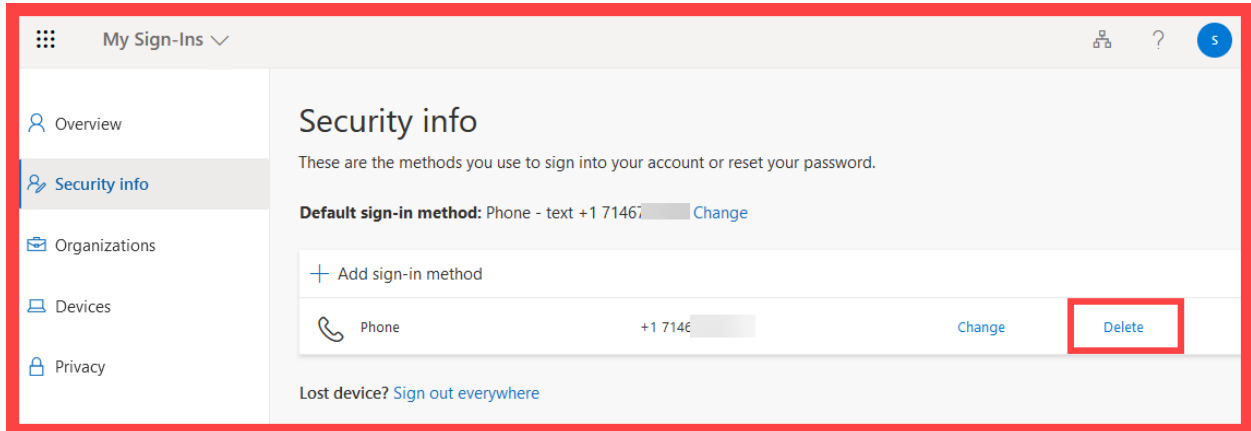
This will initiate the process for Adding another method.

Your choices are:

- **Authenticator app**
  - See [Microsoft Authenticator](#) or [Google Authenticator](#) setup steps.
- **Phone or Alternate Phone**
  - See [SMS Text Message](#) or [Phone Call](#) setup steps.

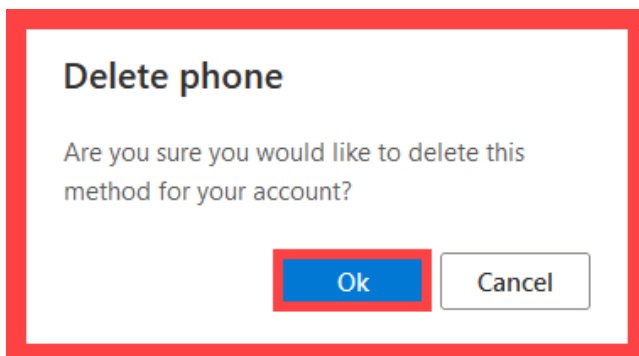
## Step 3b - Delete a sign-in method

To **delete a sign-in method**, locate it on the list, and select **Delete** next to that sign-in method.

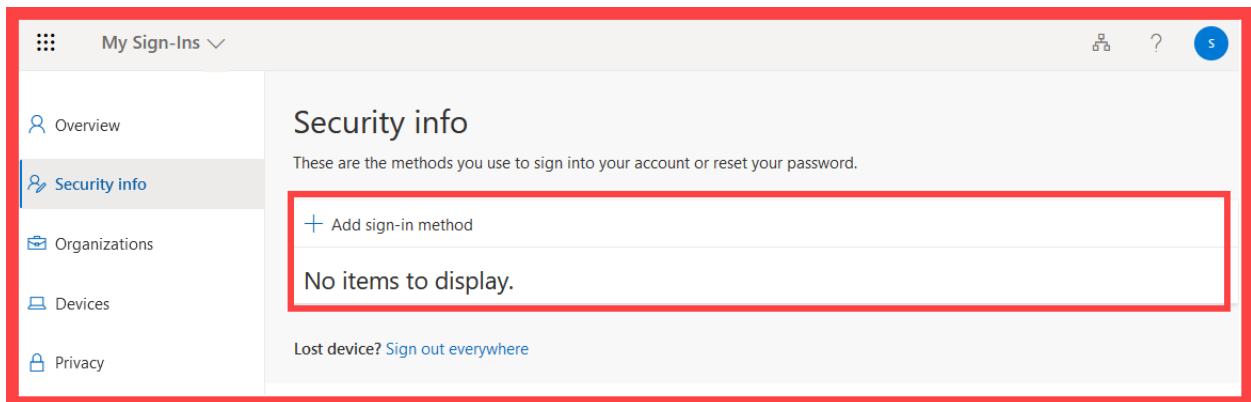


A prompt will ask, *“Are you sure you would like to delete this method for your account?”*

Select **Ok** to continue.

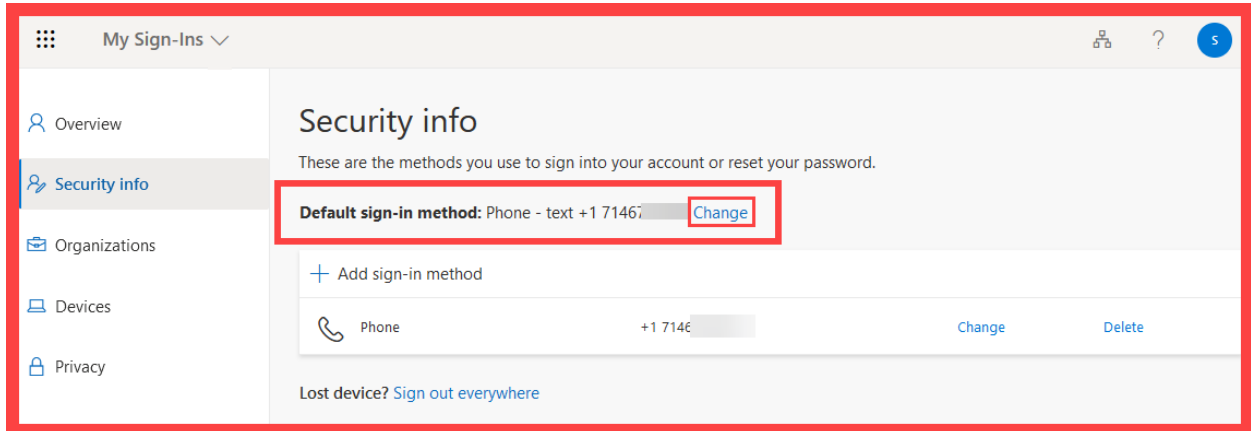


Lastly, check the **Security info** page to confirm the sign-in method was deleted.

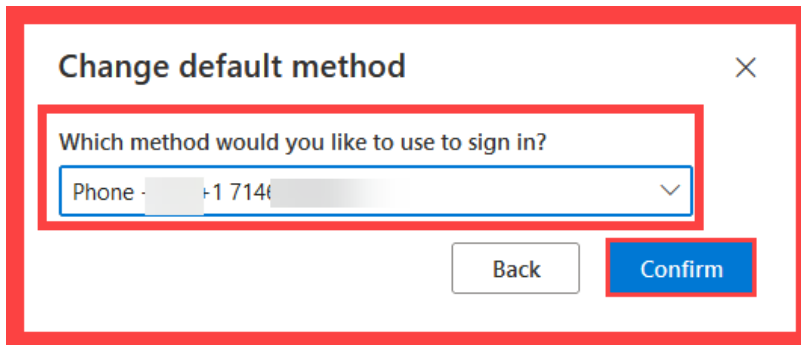


## Step 3c - Change Default sign-in method

To change your **Default sign-in method**, select **Change** next to Default sign-in method.



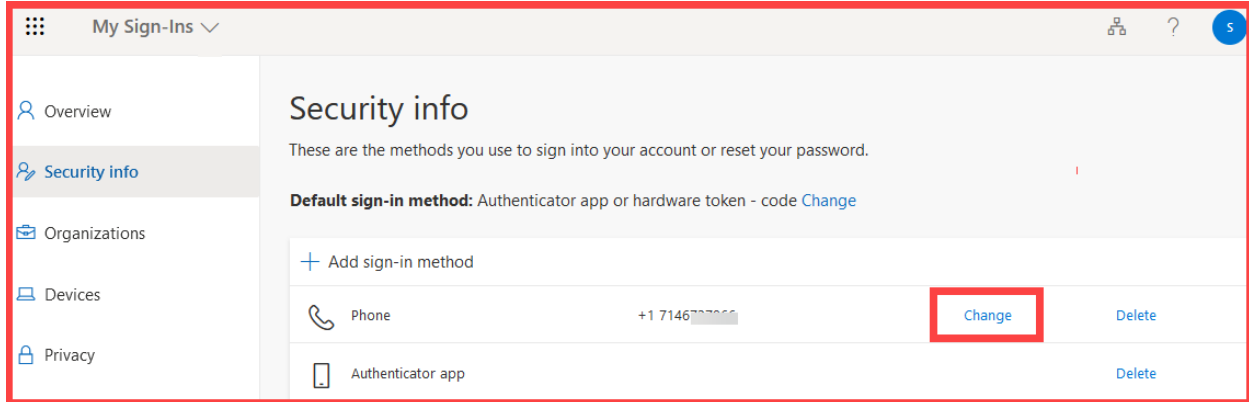
Select another method from the dropdown list, then select **Confirm**.



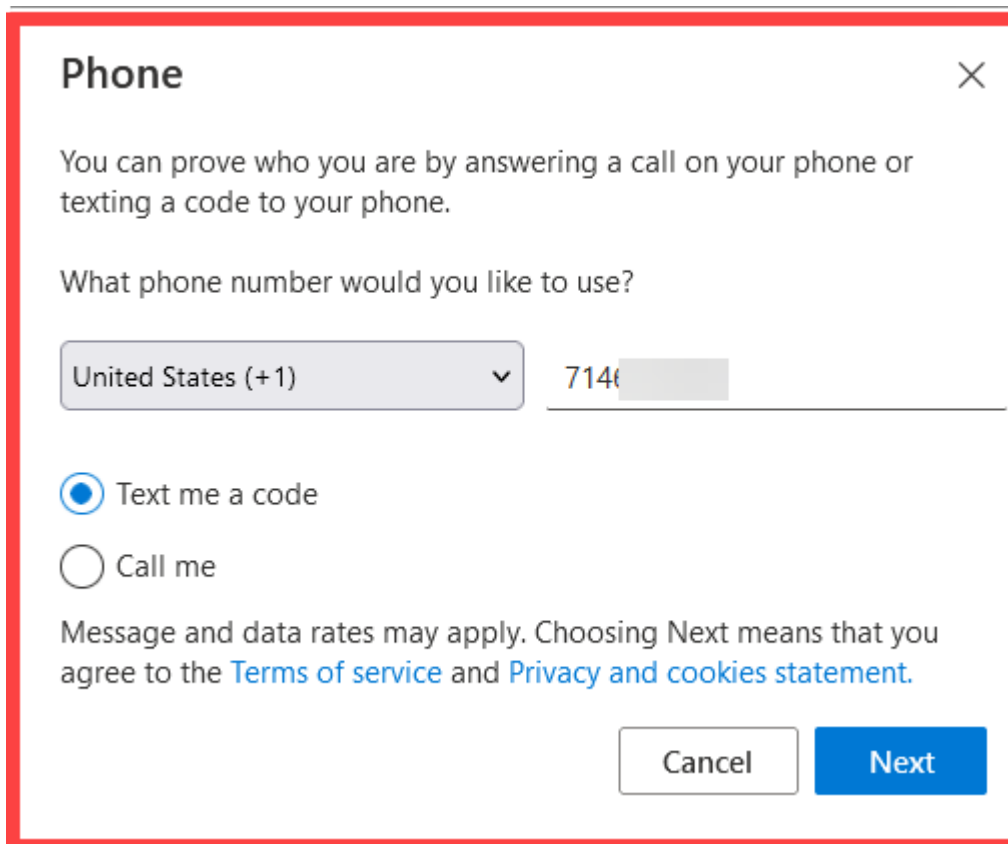
*NOTE: You need at least two sign-in methods added to change the Default sign-in method to something else.*

## Step 3d - Change an existing sign-in method

To change an existing sign-in method (e.g., phone number), locate it on the list, and select **Change** next to that sign-in method.

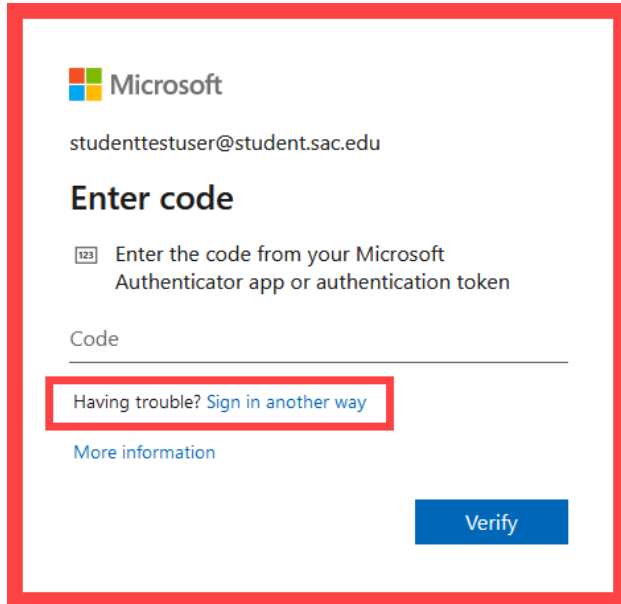


If changing a phone number, you may be prompted to re-authenticate through a text or phone call. Continue through the prompts to set up the new phone number.



## Step 3e - Sign in with an Alternative Method

Once you setup two or more Authentication Methods, you can select the link for **Sign in another way** at the login screen to **use another authentication method**.



Microsoft  
studenttestuser@student.sac.edu

### Enter code

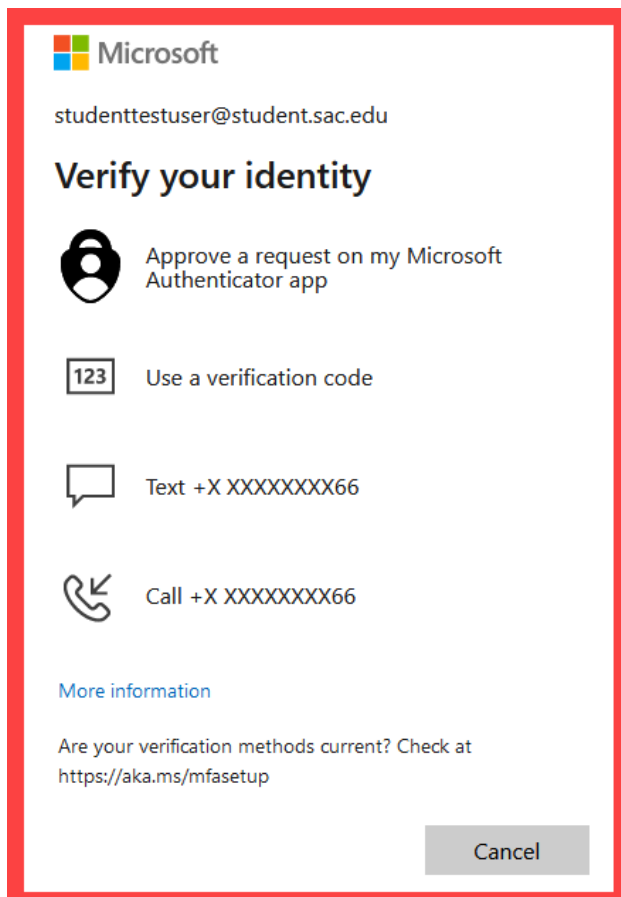
123 Enter the code from your Microsoft Authenticator app or authentication token

Code

Having trouble? [Sign in another way](#)


[More information](#)

Verify





Microsoft  
studenttestuser@student.sac.edu

### Verify your identity

 Approve a request on my Microsoft Authenticator app

123 Use a verification code

 Text +X XXXXXXXX66

 Call +X XXXXXXXX66

[More information](#)

Are your verification methods current? Check at <https://aka.ms/mfasetup>

Cancel

## Troubleshooting problems

### Troubleshooting sign-in problems

Use the [Password Reset page](#) if you have forgotten your password or need to retrieve your username.

Use the [Change Password page](#) to create a new password.

Read the [Single Sign-On FAQs \(Frequently Asked Questions\) page](#) for other sign in issues.

Read the [Account Lockout Troubleshooting](#) guide.

### Troubleshooting other problems

See Microsoft's video guide on YouTube, for [How to register for Azure Multi-Factor Authentication](#).

### Receiving Help

**Faculty and Staff** may contact the **ITS (Information Technology Services) Help Desk** for further assistance:

- Website: [ITS Help Desk page](#)
- Submit a Ticket: <https://rscdd.edu/helpdesk>
- Phone: **714-564-4357 Extension 0**
- Email: [itshelpdesk@rscdd.edu](mailto:itshelpdesk@rscdd.edu).

*[\(Select this link to return to the beginning of the document\)](#)*