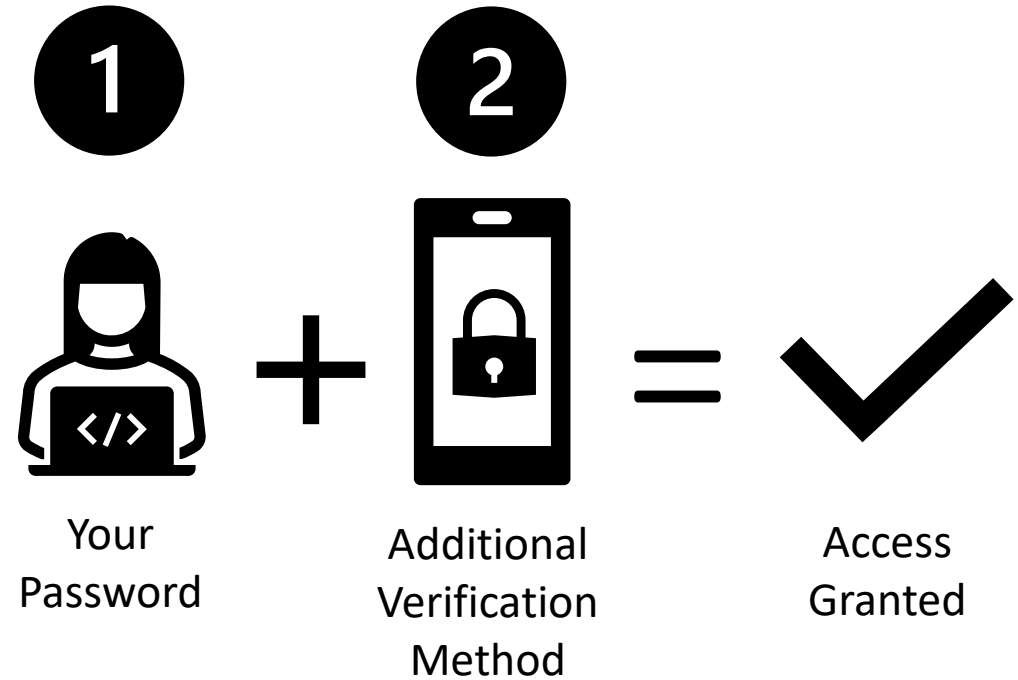


Multi-Factor Authentication (MFA) for Single Sign-on (SSO)



What is MFA?

- **Multi-factor authentication (MFA)** means using **at least 2 factors** to **verify your identity**.



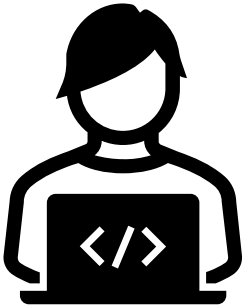
Multi-factor authentication adds an extra layer of security to **protect your online accounts** against **cyber criminals**.

Examples of MFA



Example 1:

Your bank sends a **text message** to your phone with a **verification code** to confirm your **online banking login**.

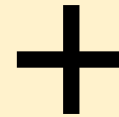


Example 2:

A website sends a **Push Notification** to your phone asking to **approve** your **sign-in to a new device**.

These examples use at least **2** authentication factors:

1. Your password (i.e., something you **know**)



2. Your phone (i.e., something you **own**)

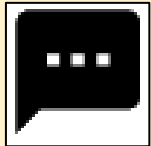
Approved Methods for MFA:



[Microsoft Authenticator \(*Recommended\)](#)



[Google Authenticator](#)



[SMS Text Message](#)



[Phone Call](#)



[Hardware Token](#)

Initial Setup Prompt

STEP 1 – Login to [Office.com](https://aka.ms/mfasetup) with your Single Sign-on (SSO) username.

STEP 2 – On “More Information required” screen, select Next.

NOTE:

Go to <https://aka.ms/mfasetup> to manually initiate the MFA setup process.

The image shows two overlapping screenshots of login pages. The top screenshot is the Microsoft Sign in page, which includes the Microsoft logo, the text "Sign in", a text input field containing "studenttestuser@student.sac.edu", and links for "No account? Create one!" and "Can't access your account?". At the bottom are "Back" and "Next" buttons. The "Next" button is highlighted with a red border. The bottom screenshot is the Santa Ana College login page. It features a red header with the college's name and logo. Below the header is a sign-in form with a text input field for the username "studenttestuser@student.sac.edu" and a password input field with masked characters. There is a "Keep me signed in" checkbox and a "Sign in" button. Below the form, there is a message about changing login authentication screens and links to "Learn More - Single Sign-On FAQs" and "Retrieve Username or Reset Password". At the bottom, there are email addresses for students and employees, with an example provided for each.

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

Santa Ana College
SANTA ANA 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@rscdd.edu
Example: Smith_John@rscdd.edu

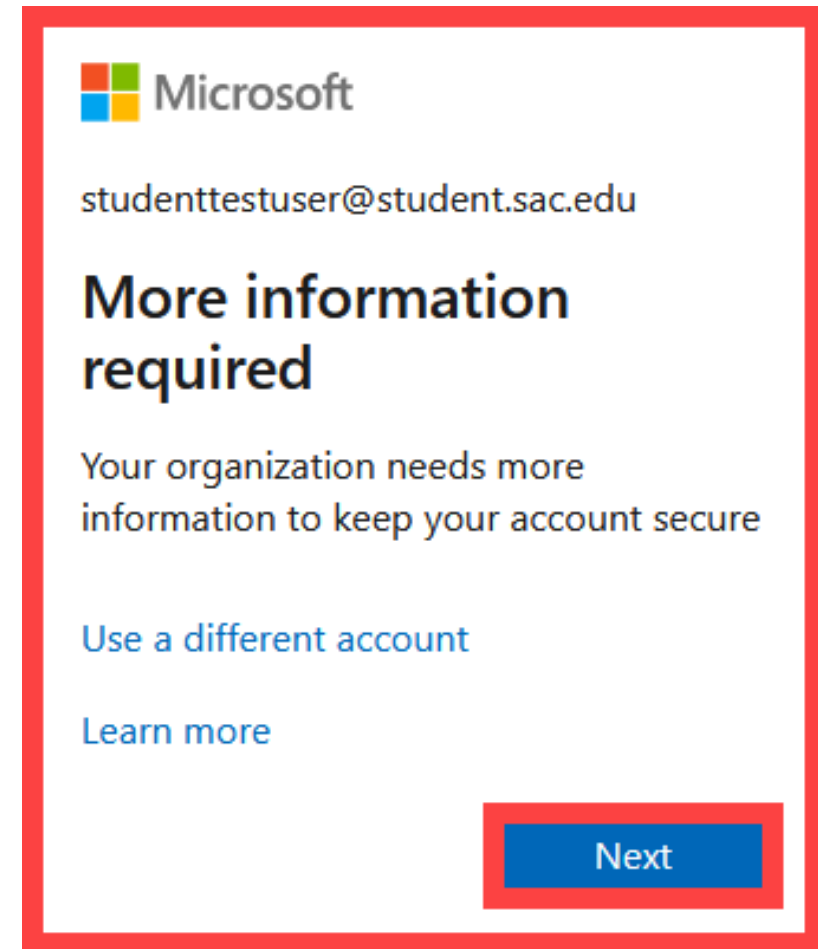
Initial Setup Prompt

STEP 1 – Login to Office.com with your Single Sign-on (SSO) username

STEP 2 – On “More Information required” screen, select Next.

NOTE:

Go to <https://aka.ms/mfasetup> to manually initiate the MFA setup process.





Microsoft Authenticator (*Recommended)

STEP 1 – Login to Office.com with your Single Sign-On (SSO) Username.

STEP 2 – Install the Microsoft Authenticator App on your Phone.

STEP 3 – Scan the QR code from the Microsoft Authenticator app.

STEP 4 – Verify the Mobile App registered successfully.

STEP 5 – Complete setup and Office.com login.

STEP 6 – Verify your identity with Microsoft Authenticator on next login.

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@rscdd.edu
- Example: Smith_John@rscdd.edu

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 Authenticator (*Recommended)

STEP 1 – Login to Office.com with your Single Sign-On (SSO) Username.

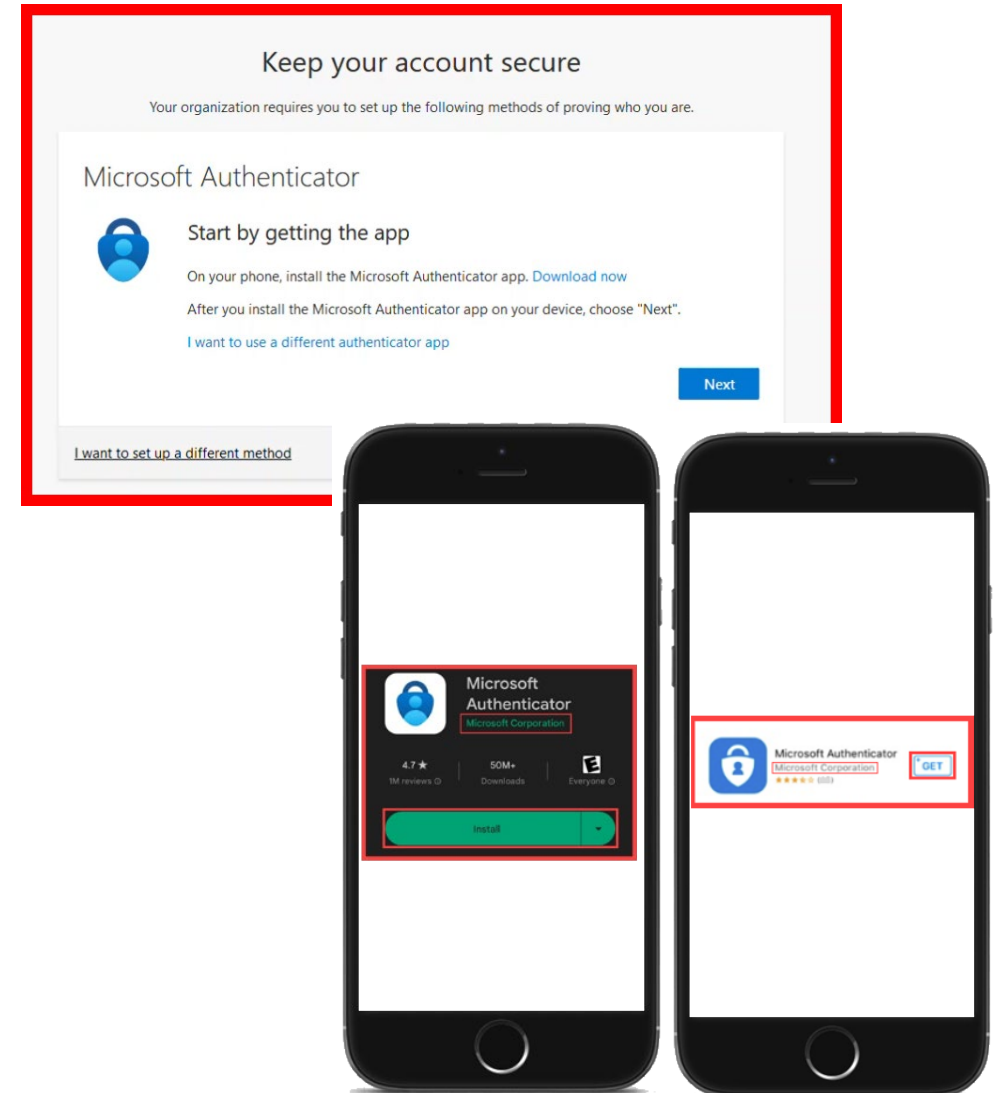
STEP 2 – Install the Microsoft Authenticator App on your Phone.

STEP 3 – Scan the QR code from the Microsoft Authenticator app.

STEP 4 – Verify the Mobile App registered successfully.

STEP 5 – Complete setup and Office.com login.

STEP 6 – Verify your identity with Microsoft Authenticator on next login.





Microsoft Authenticator (*Recommended)

STEP 1 – Login to Office.com with your Single Sign-On (SSO) Username.

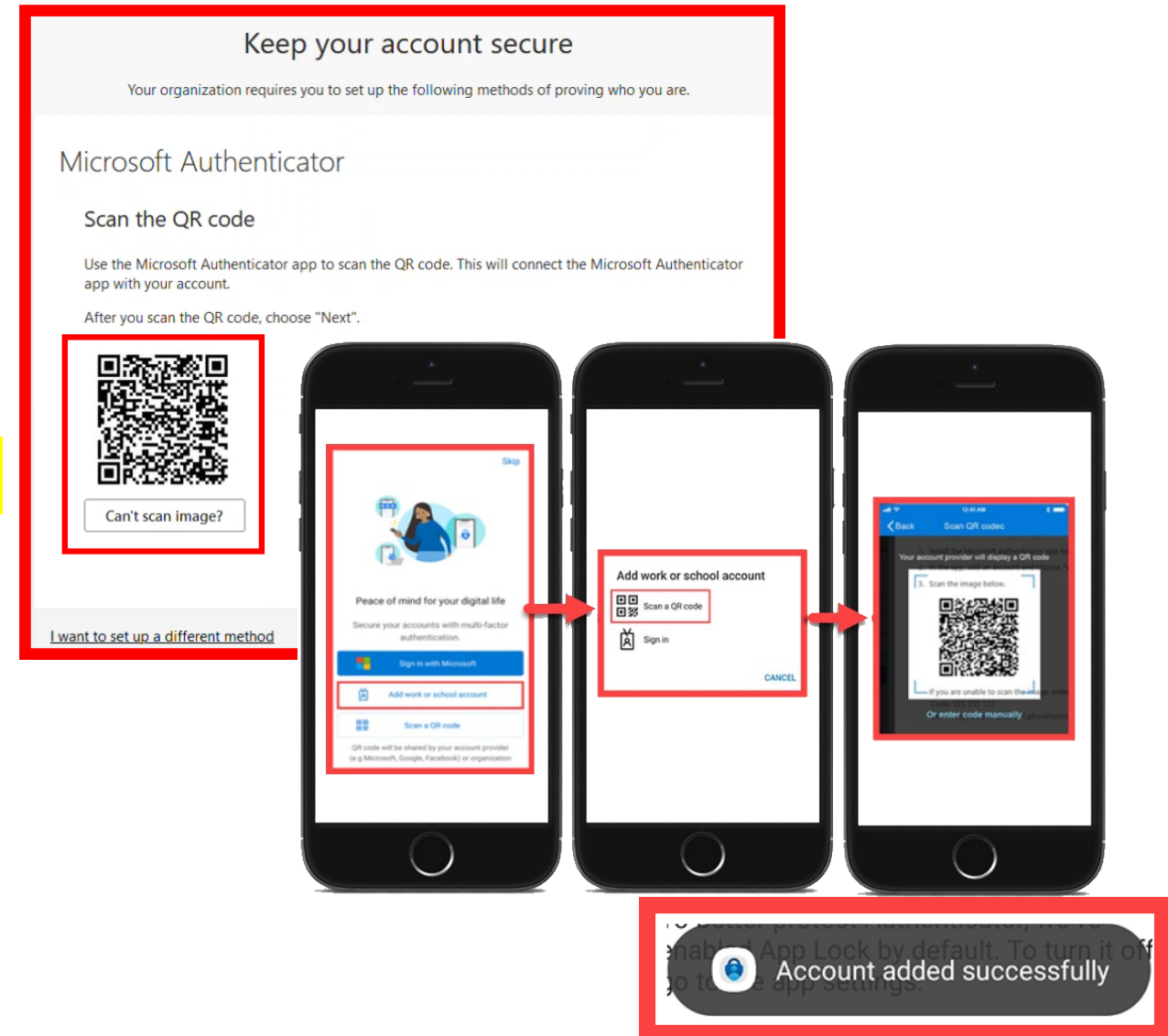
STEP 2 – Install the Microsoft Authenticator App on your Phone.

STEP 3 – Scan the QR code from the Microsoft Authenticator app.

STEP 4 – Verify the Mobile App registered successfully.

STEP 5 – Complete setup and Office.com login.

STEP 6 – Verify your identity with Microsoft Authenticator on next login.





Microsoft Authenticator (*Recommended)

STEP 1 – Login to Office.com with your Single Sign-On (SSO) Username.

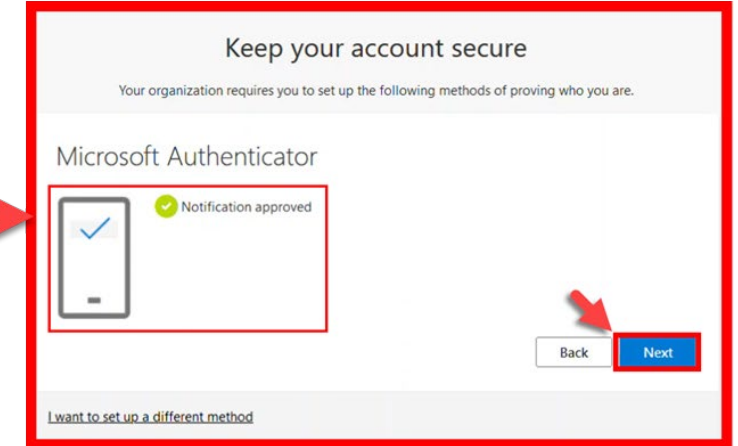
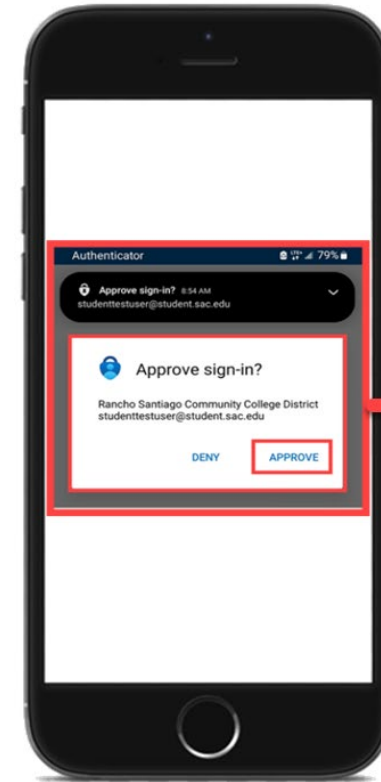
STEP 2 – Install the Microsoft Authenticator App on your Phone.

STEP 3 – Scan the QR code from the Microsoft Authenticator app.

STEP 4 – Verify the Mobile App registered successfully.

STEP 5 – Complete setup and Office.com login.

STEP 6 – Verify your identity with Microsoft Authenticator on next login.





Microsoft Authenticator (*Recommended)

STEP 1 – Login to Office.com with your Single Sign-On (SSO) Username.

STEP 2 – Install the Microsoft Authenticator App on your Phone.

STEP 3 – Scan the QR code from the Microsoft Authenticator app.

STEP 4 – Verify the Mobile App registered successfully.

STEP 5 – Complete setup and Office.com login.

STEP 6 – Verify your identity with Microsoft Authenticator on next login.

The image shows two overlapping screenshots of a Microsoft account setup process, both outlined in red. The top screenshot is titled "Keep your account secure" and states "Your organization requires you to set up the following methods of proving who you are." It shows a "Success!" message: "Great job! You have successfully set up your security info. Choose 'Done' to continue signing in." Under "Default sign-in method:", there is a Microsoft Authenticator icon and the text "Microsoft Authenticator". A red arrow points to a blue "Done" button. The bottom screenshot is a Microsoft sign-in confirmation screen for "studenttestuser@student.sac.edu". It asks "Stay signed in?" with the text "Do this to reduce the number of times you are asked to sign in." There is an unchecked checkbox for "Don't show this again" and two buttons at the bottom: a grey "No" button and a blue "Yes" button.



Microsoft Authenticator (*Recommended)

STEP 1 – Login to Office.com with your Single Sign-On (SSO) Username.

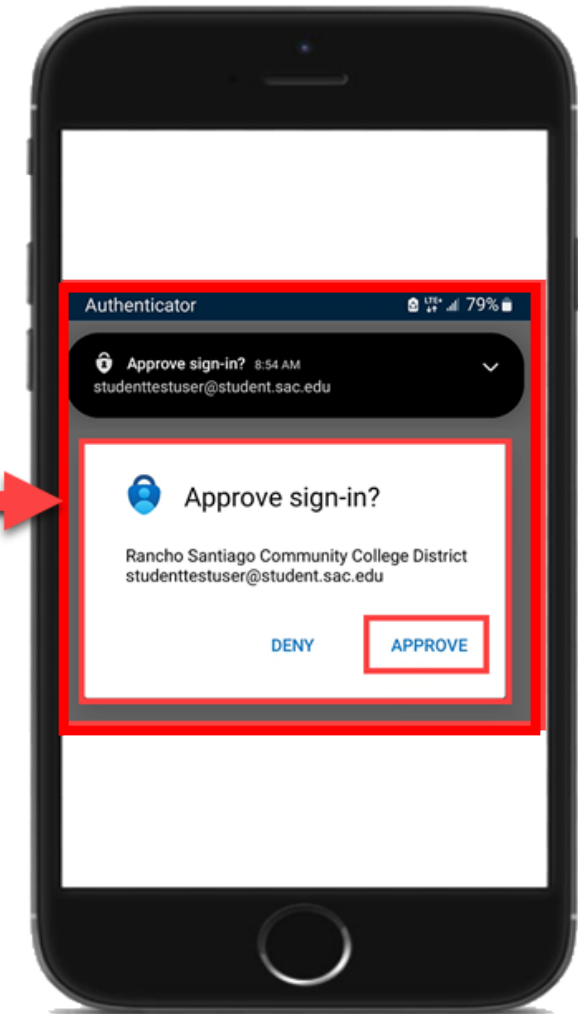
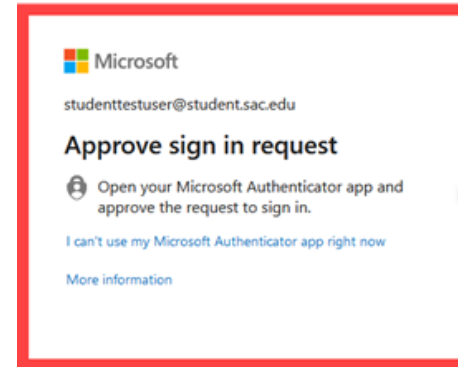
STEP 2 – Install the Microsoft Authenticator App on your Phone.

STEP 3 – Scan the QR code from the Microsoft Authenticator app.

STEP 4 – Verify the Mobile App registered successfully.

STEP 5 – Setup a Secondary Verification Method.

STEP 6 – Verify your identity with Microsoft Authenticator on next login.





Google Authenticator

STEP 1 – Login to Office.com with your Single Sign-On (SSO) username.

STEP 2 – Select “I want to use a different authenticator app”.

STEP 3 – Download and install the Google Authenticator app.

STEP 4 – Set up your account and scan the QR code.

STEP 5 – Verify the Google Authenticator app works.

STEP 6 – Complete setup and Office.com login.

STEP 7 – Verify your identity with Google Authenticator on next login.

The screenshot shows the Office.com login page for Santa Ana College. On the left is a vertical banner with logos for Santa Ana College, Rancho Santiago Community College District, and Santiago Canyon College. The main content area has the heading "Sign in with your organizational account" and a login form with fields for "studenttestuser@student.sac.edu" and a password. Below the password field is a checkbox for "Keep me signed in" and a blue "Sign in" button. Further down, there is a section for "Login authentication screen" with links for "Learn More - Single Sign-On" and "Retrieve Username or Password". It lists email formats for students and employees. A red-bordered box on the right contains a Microsoft message: "More information required" and "Your organization needs more information to keep your account secure". It includes links for "Use a different account" and "Learn more", and a blue "Next" button at the bottom right.

Sign in with your organizational account

studenttestuser@student.sac.edu

Keep me signed in

Sign in

Login authentication screen
[Learn More - Single Sign-On](#)
[Retrieve Username or Password](#)

For Students:

- SelfServiceID@student.sac.edu
- SelfServiceID@student.sac.edu
- Example: ab12345@student.sac.edu

For Employees:

- LastName_FirstName@scsac.edu
- LastName_FirstName@sac.edu
- LastName_FirstName@rscsac.edu
- Example: Smith_John@rscsac.edu

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



Google Authenticator

STEP 1 – Login to Office.com with your Single Sign-On (SSO) username.

STEP 2 – Select “I want to use a different authenticator app”.

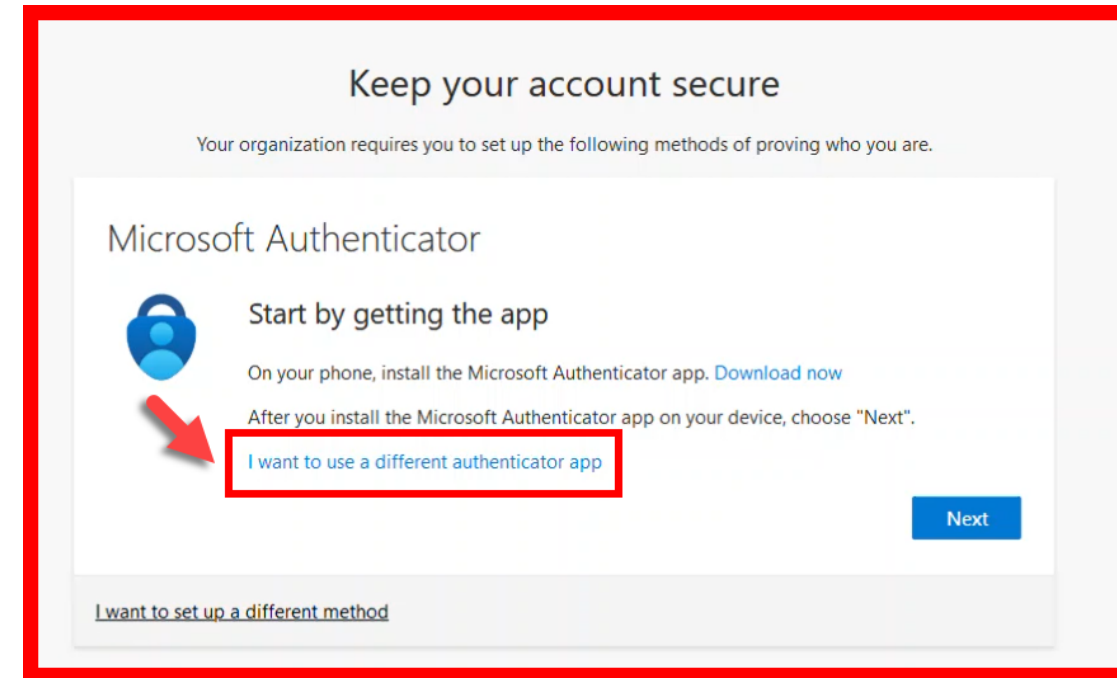
STEP 3 – Download and install the Google Authenticator app.

STEP 4 – Set up your account and scan the QR code.

STEP 5 – Verify the Google Authenticator app works.

STEP 6 – Complete setup and Office.com login

STEP 7 – Verify your identity with Google Authenticator on next login





Google Authenticator

STEP 1 – Login to Office.com with your Single Sign-On (SSO) username.

STEP 2 – Select “I want to use a different authenticator app”.

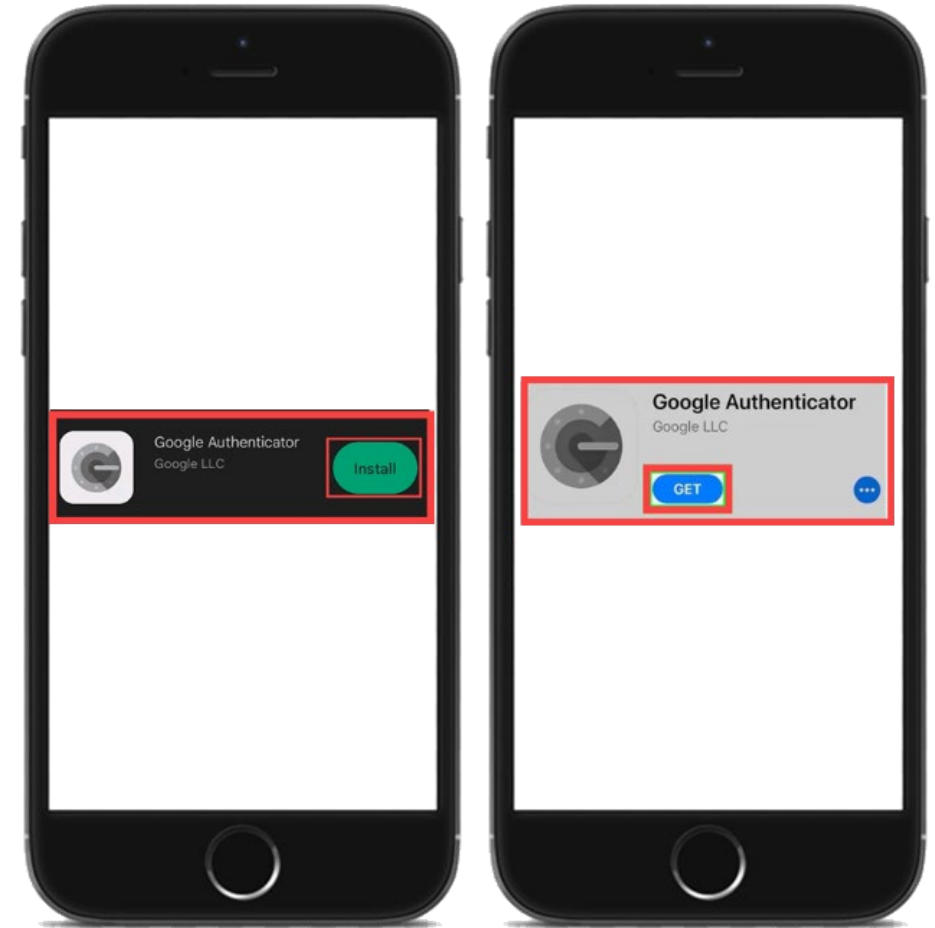
STEP 3 – Download and install the Google Authenticator app.

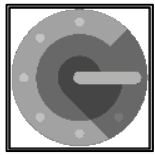
STEP 4 – Set up your account and scan the QR code.

STEP 5 – Verify the Google Authenticator app works.

STEP 6 – Complete setup and Office.com login.

STEP 7 – Verify your identity with Google Authenticator on next login.





Google Authenticator

STEP 1 – Login to Office.com with your Single Sign-On (SSO) username.

STEP 2 – Select “I want to use a different authenticator app”.

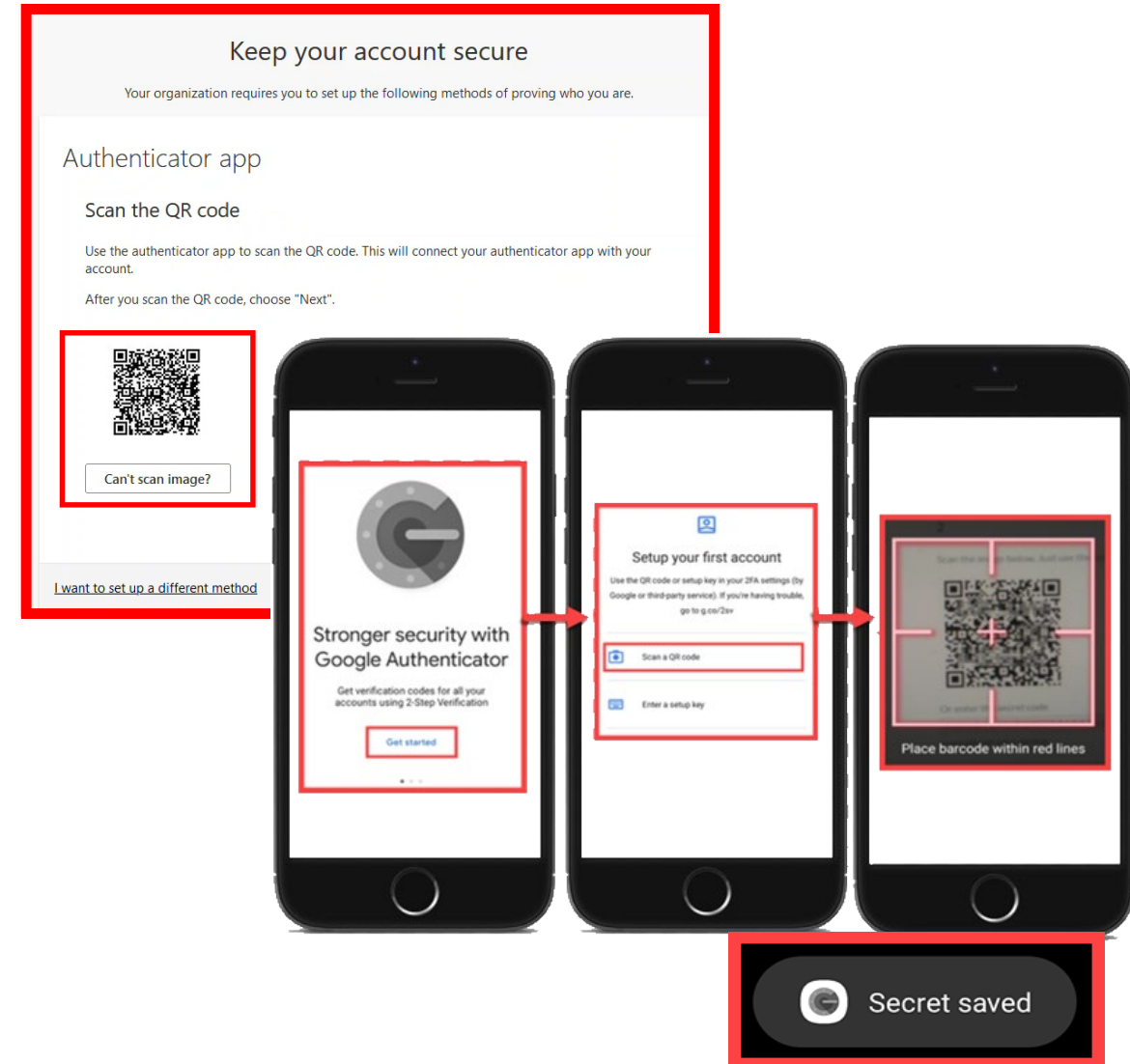
STEP 3 – Download and install the Google Authenticator app.

STEP 4 – Set up your account and scan the QR code.

STEP 5 – Verify the Google Authenticator app works.

STEP 6 – Complete setup and Office.com login.

STEP 7 – Verify your identity with Google Authenticator on next login.





Google Authenticator

STEP 1 – Login to Office.com with your Single Sign-On (SSO) username.

STEP 2 – Select “I want to use a different authenticator app”.

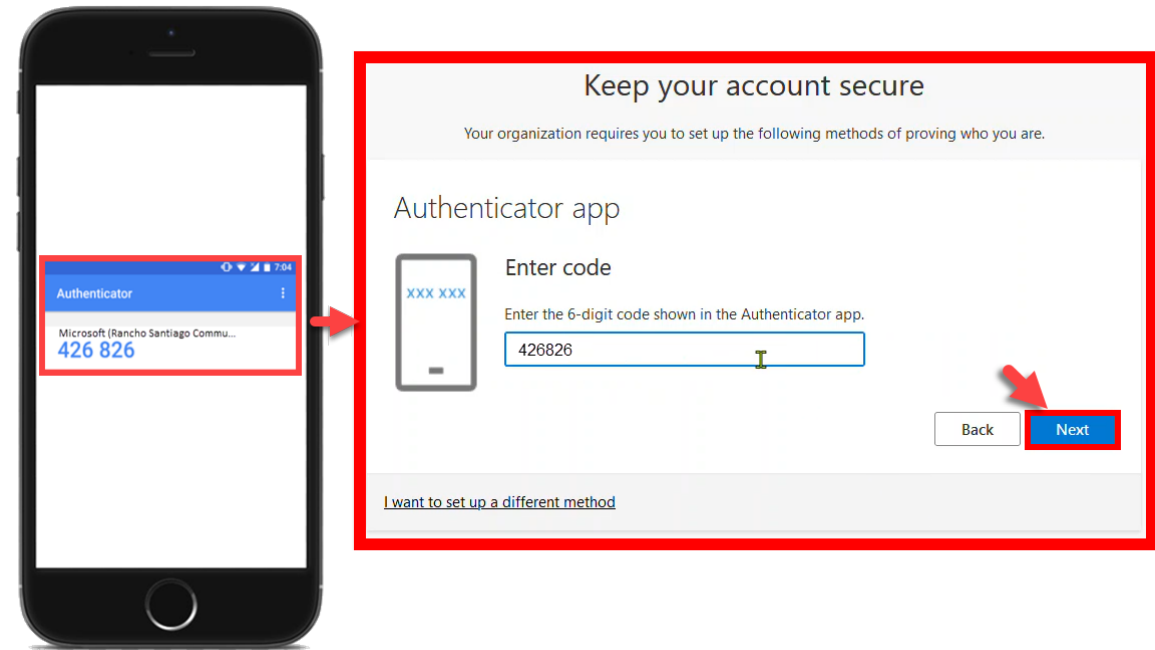
STEP 3 – Download and install the Google Authenticator app.

STEP 4 – Set up your account and scan the QR code.

STEP 5 – Verify the Google Authenticator app works.

STEP 6 – Complete setup and Office.com login.

STEP 7 – Verify your identity with Google Authenticator on next login.





Google Authenticator

STEP 1 – Login to Office.com with your Single Sign-On (SSO) username.

STEP 2 – Select “I want to use a different authenticator app”.

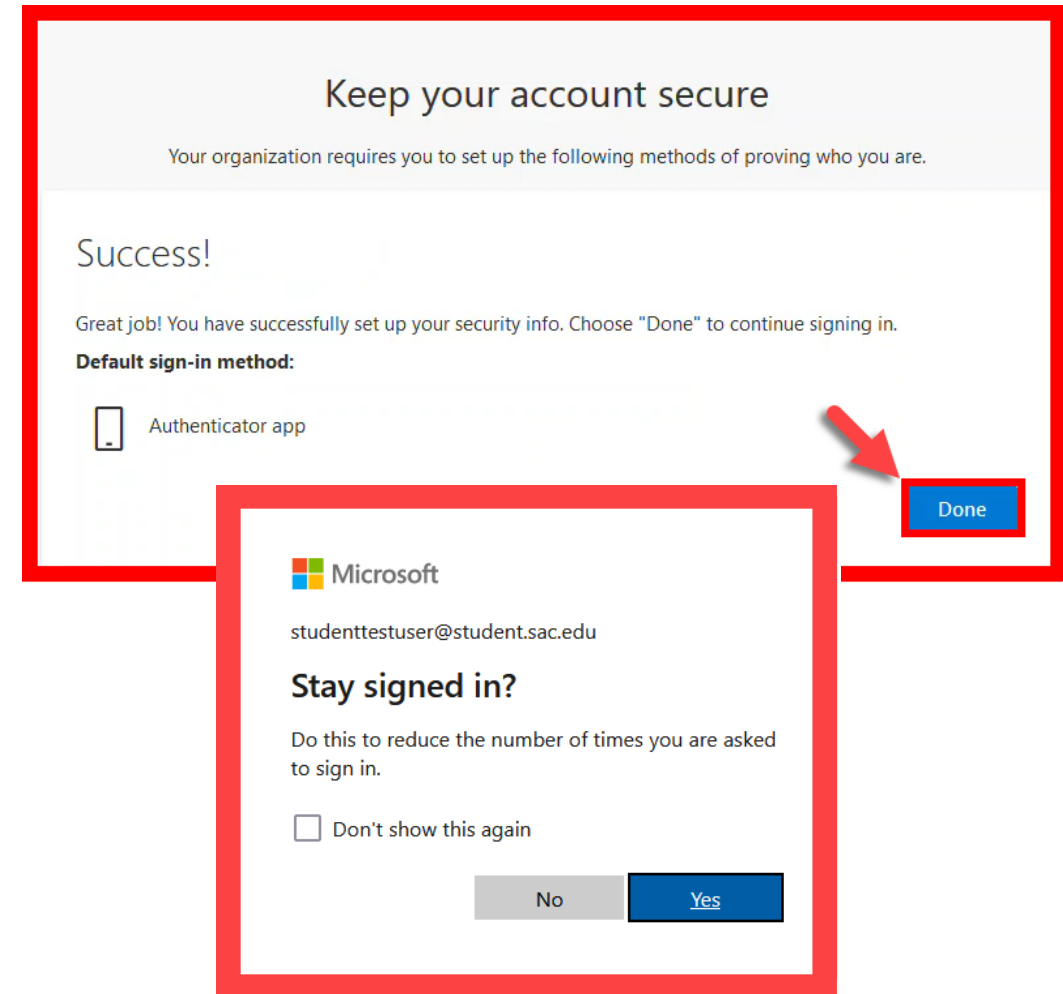
STEP 3 – Download and install the Google Authenticator app.

STEP 4 – Set up your account and scan the QR code.

STEP 5 – Verify the Google Authenticator app works.

STEP 6 – Complete setup and Office.com login.

STEP 7 – Verify your identity with Google Authenticator on next login.





Google Authenticator

STEP 1 – Login to Office.com with your Single Sign-On (SSO) username.

STEP 2 – Select “I want to use a different authenticator app”.

STEP 3 – Download and install the Google Authenticator app.

STEP 4 – Set up your account and scan the QR code.

STEP 5 – Verify the Google Authenticator app works.

STEP 6 – Complete setup and Office.com login

STEP 7 – Verify your identity with Google Authenticator on next login.

Microsoft
studenttestuser@student.sac.edu

Enter code

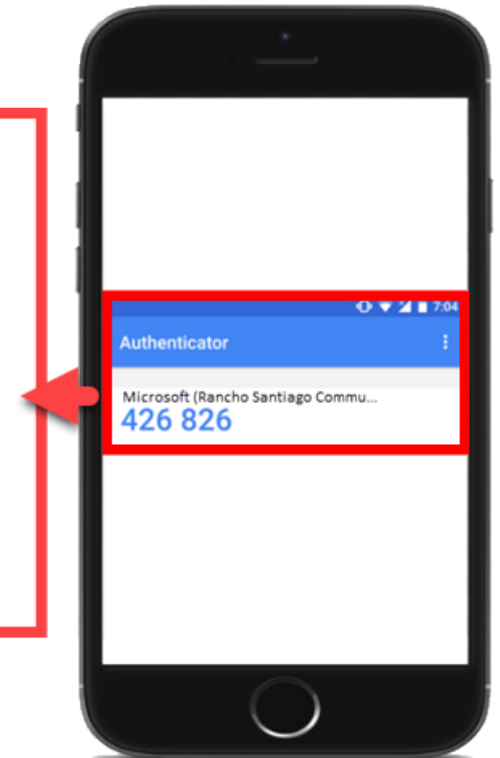
Enter the code displayed in the authenticator app on your mobile device

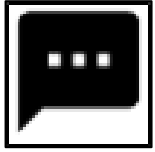
426826

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

[More information](#)

Verify





SMS Text Message

STEP 1 – Login to Office.com with your Single Sign-On (SSO) username.

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

STEP 3 – Enter phone number, then select “Text me a code”.

STEP 4 – Enter verification code sent through SMS text to your phone.

STEP 5 – Complete setup and Office.com login.

STEP 6 – Verify your identity with SMS Text Message on next login.

The screenshot displays the Office.com login interface for Santa Ana College. On the left, a vertical banner features the college's logo and name. The main login area includes a 'Sign in with your organizational account' section with a text input field containing 'studenttestuser@student.sac.edu' and a password field with masked characters. A 'Keep me signed in' checkbox and a 'Sign in' button are also present. Below this, a 'Login authentication screen' section provides instructions for students and employees, listing email formats and examples. A red-bordered box highlights a Microsoft security warning on the right side of the page, stating 'More information required' and 'Your organization needs more information to keep your account secure'. It offers links for 'Use a different account' and 'Learn more', and a 'Next' button at the bottom right.

Sign in with your organizational account

studenttestuser@student.sac.edu

Keep me signed in

Sign in

Login authentication screen
[Learn More - Single Sign-On](#)
[Retrieve Username or Password](#)

For Students:

- SelfServiceID@student.sac.edu
- SelfServiceID@student.sac.edu
- Example: ab12345@student.sac.edu

For Employees:

- LastName_FirstName@sc.edu
- LastName_FirstName@sac.edu
- LastName_FirstName@rsc.edu
- Example: Smith_John@rsc.edu

Microsoft

studenttestuser@student.sac.edu

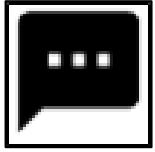
More information required

Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

Next



SMS Text Message

STEP 1 – Login to Office.com with your Single Sign-On (SSO) username.

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

STEP 3 – Enter phone number, then select “Text me a code”.

STEP 4 – Enter verification code sent through SMS text to your phone.

STEP 5 – Complete setup and Office.com login.

STEP 6 – Verify your identity with SMS Text Message on next login.

The image shows a screenshot of the Microsoft Authenticator setup interface. The main window is titled "Keep your account secure" and contains instructions for setting up the app. A red arrow points to a link at the bottom left that says "I want to set up a different method". A second, smaller window is overlaid on top, titled "Choose a different method". This window asks "Which method would you like to use?" and has a dropdown menu with "Phone" selected. At the bottom of this window are "Cancel" and "Confirm" buttons. The "Confirm" button is highlighted with a red box and a green mouse cursor icon. The entire setup process is outlined with red borders to indicate the steps to follow.

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

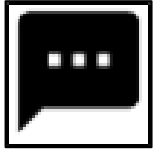
[I want to set up a different method](#)

Choose a different method ×

Which method would you like to use?

Phone

Cancel Confirm



SMS Text Message

STEP 1 – Login to Office.com with your Single Sign-On (SSO) username.

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

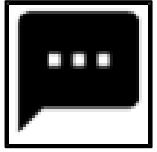
STEP 3 – Enter phone number, then select “Text me a code”.

STEP 4 – Enter verification code sent through SMS text to your phone.

STEP 5 – Complete setup and Office.com login.

STEP 6 – Verify your identity with SMS Text Message on next login.

A screenshot of a web form titled "Keep your account secure". Below the title is a subtitle: "Your organization requires you to set up the following methods of proving who you are." The main heading is "Phone". Below this is a descriptive sentence: "You can prove who you are by answering a call on your phone or texting a code to your phone." The question is "What phone number would you like to use?". There is a dropdown menu for the country, currently showing "United States (+1)", and a text input field for the phone number, which contains "7146". Below the phone number field are two radio button options: "Text me a code" (which is selected) and "Call me". Below these options is a line of text: "Message and data rates may apply. Choosing Next means that you agree to the Terms of service and Privacy and cookies statement." At the bottom right is a blue "Next" button, which is highlighted with a red arrow. At the bottom left is a link that says "I want to set up a different method". The entire form is enclosed in a red border.



SMS Text Message

STEP 1 – Login to Office.com with your Single Sign-On (SSO) username.

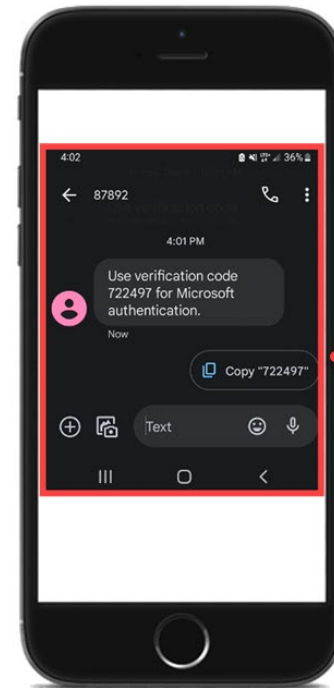
STEP 2 – Select “I want to set up a different method,” then select Phone.

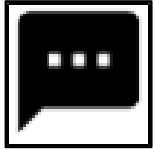
STEP 3 – Enter phone number, then select “Text me a code”.

STEP 4 – Enter verification code sent through SMS text to your phone.

STEP 5 – Complete setup and Office.com login.

STEP 6 – Verify your identity with SMS Text Message on next login.

A screenshot of the Microsoft account security setup page. The title is "Keep your account secure" with a subtitle "Your organization requires you to set up the following methods of proving who you are." Under the heading "Phone", there is a text input field containing "722497". Above the field is a label "We just sent a 6 digit code to +1 714" and a prompt "Enter the code below." Below the field is a "Resend code" link. At the bottom right are "Back" and "Next" buttons, with a red arrow pointing to the "Next" button. At the bottom left is a link "I want to set up a different method".



SMS Text Message

STEP 1 – Login to Office.com with your Single Sign-On (SSO) username.

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

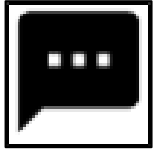
STEP 3 – Enter phone number, then select “Text me a code”.

STEP 4 – Enter verification code sent through SMS text to your phone.

STEP 5 – Complete setup and Office.com login

STEP 6 – Verify your identity with SMS Text Message on next login.

The image shows two overlapping screenshots from a Microsoft account interface, both outlined with a thick red border. The top screenshot is titled "Keep your account secure" and states "Your organization requires you to set up the following methods of proving who you are." It shows a "Success!" message: "Great job! You have successfully set up your security info. Choose 'Done' to continue signing in." Below this, it says "Default sign-in method:" and shows a phone icon with the number "+1 7146" in a greyed-out field. A red arrow points to a blue "Done" button in the bottom right corner. The bottom screenshot is a Microsoft sign-in prompt for the user "studenttestuser@student.sac.edu". It asks "Stay signed in?" with the instruction "Do this to reduce the number of times you are asked to sign in." There is a checkbox labeled "Don't show this again" which is currently unchecked. At the bottom are two buttons: a grey "No" button and a blue "Yes" button.



SMS Text Message

STEP 1 – Login to Office.com with your Single Sign-On (SSO) username

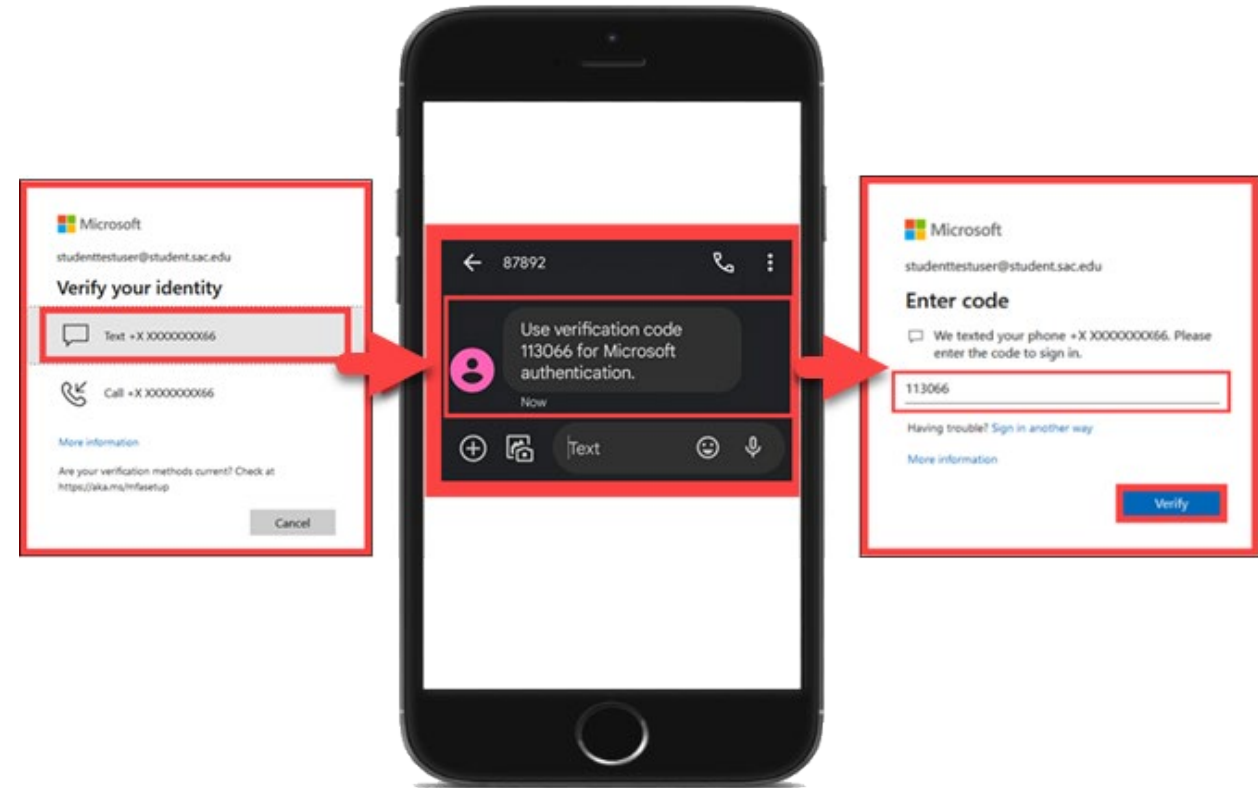
STEP 2 – Select “I want to set up a different method,” then select Phone.

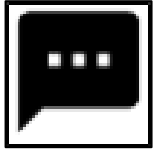
STEP 3 – Enter phone number, then select “Text me a code”

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

STEP 5 – Complete setup and Office.com login

STEP 6 – Verify your identity with SMS Text Message on next login.





Phone Call

STEP 1 – Login to Office.com with your Single Sign-On (SSO) username

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

STEP 3 – Enter phone number, then select “Call Me”

STEP 4 – Answer the phone call from Microsoft and press # key to verify

STEP 5 – Complete setup and Office.com login

STEP 6 – Verify your identity with Phone call on next login.

The screenshot displays the Office.com login interface. On the left, there are logos for Santa Ana College, Rancho Santiago Community College District, and Santiago Canyon College. The main content area prompts the user to 'Sign in with your organizational account' with a text input field containing 'studenttestuser@student.sac.edu' and a password field with masked characters. A 'Sign in' button is highlighted with a red box. Below the login fields, there is a 'Keep me signed in' checkbox and a 'Login authentication screen' section with links for 'Learn More - Single Sign-On' and 'Retrieve Username or Reset Password'. For students, it lists email formats like 'SelfServiceID@student.sac.edu' and 'Example: ab12345@student.sac.edu'. For employees, it lists email formats like 'LastName_FirstName@sac.edu' and 'Example: Smith_John@rsc.edu'. A red-bordered overlay on the right side of the page contains the Microsoft logo, the same email address, and the heading 'More information required'. It states 'Your organization needs more information to keep your account secure' and includes links for 'Use a different account' and 'Learn more'. A 'Next' button is located at the bottom right of this overlay.



Phone Call

STEP 1 – Login to Office.com with your Single Sign-On (SSO) username.

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

STEP 3 – Enter phone number, then select “Call Me”.

STEP 4 – Answer the phone call from Microsoft and press # key to verify.

STEP 5 – Complete setup and Office.com login.

STEP 6 – Verify your identity with Phone call on next login.

The image shows a screenshot of the Microsoft Authenticator setup interface. The main window is titled "Keep your account secure" and contains the heading "Microsoft Authenticator". It instructs the user to "Start by getting the app" and provides links for "Download now" and "I want to use a different authenticator app". A red arrow points to a link at the bottom of the window that says "I want to set up a different method". Below this, a smaller dialog box titled "Choose a different method" is shown. It asks "Which method would you like to use?" and has a dropdown menu with "Phone" selected. At the bottom of this dialog are "Cancel" and "Confirm" buttons. A red box highlights the "Confirm" button, and a green cursor icon is visible over it.



Phone Call

STEP 1 – Login to Office.com with your Single Sign-On (SSO) username.

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

STEP 3 – Enter phone number, then select “Call Me”.

STEP 4 – Answer the phone call from Microsoft and press # key to verify.

STEP 5 – Complete setup and Office.com login.

STEP 6 – Verify your identity with Phone call on next login.

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](#)



Phone Call

STEP 1 – Login to Office.com with your Single Sign-On (SSO) username.

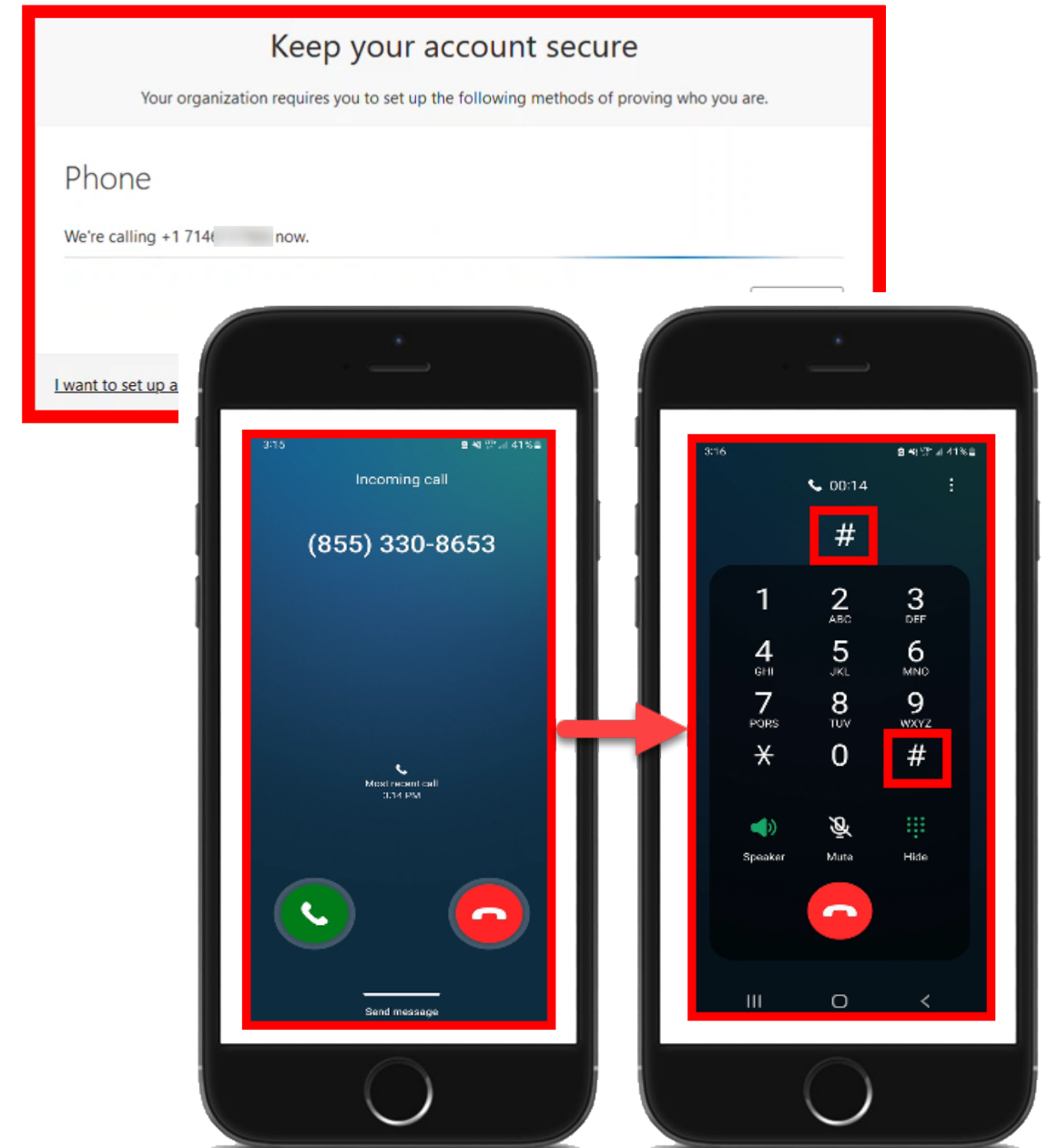
STEP 2 – Select “I want to set up a different method,” then select Phone.

STEP 3 – Enter phone number, then select “Call Me”.

STEP 4 – Answer the phone call from Microsoft and press # key to verify.

STEP 5 – Complete setup and Office.com login.

STEP 6 – Verify your identity with Phone call on next login.





Phone Call

STEP 1 – Login to Office.com with your Single Sign-On (SSO) username.

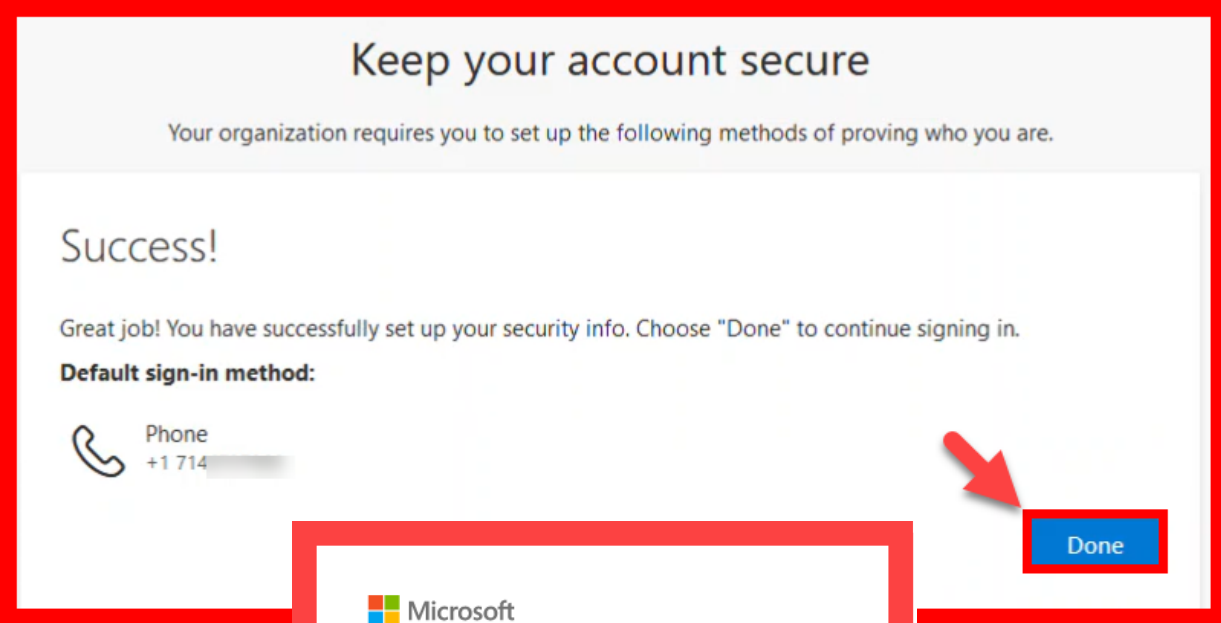
STEP 2 – Select “I want to set up a different method,” then select Phone.

STEP 3 – Enter phone number, then select “Call Me”.

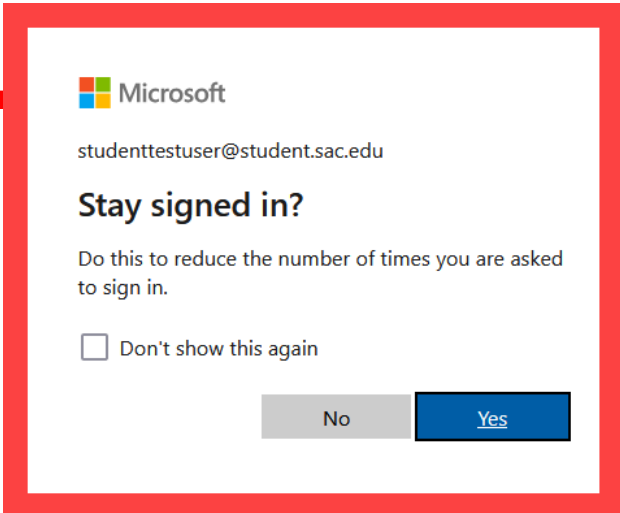
STEP 4 – Answer the phone call from Microsoft and press # key to verify.

STEP 5 – Complete setup and Office.com login.

STEP 6 – Verify your identity with Phone call on next login.



The screenshot shows a Microsoft account security setup page. At the top, it says "Keep your account secure" and "Your organization requires you to set up the following methods of proving who you are." Below this, it says "Success!" and "Great job! You have successfully set up your security info. Choose 'Done' to continue signing in." Under "Default sign-in method:", there is a phone icon and the text "Phone +1 714 [redacted]". A red arrow points to a blue "Done" button in the bottom right corner.



The dialog box shows the Microsoft logo and the email address "studenttestuser@student.sac.edu". It asks "Stay signed in?" with the text "Do this to reduce the number of times you are asked to sign in." Below this is a checkbox labeled "Don't show this again". At the bottom, there are two buttons: "No" and "Yes".



Phone Call

STEP 1 – Login to Office.com with your Single Sign-On (SSO) username.

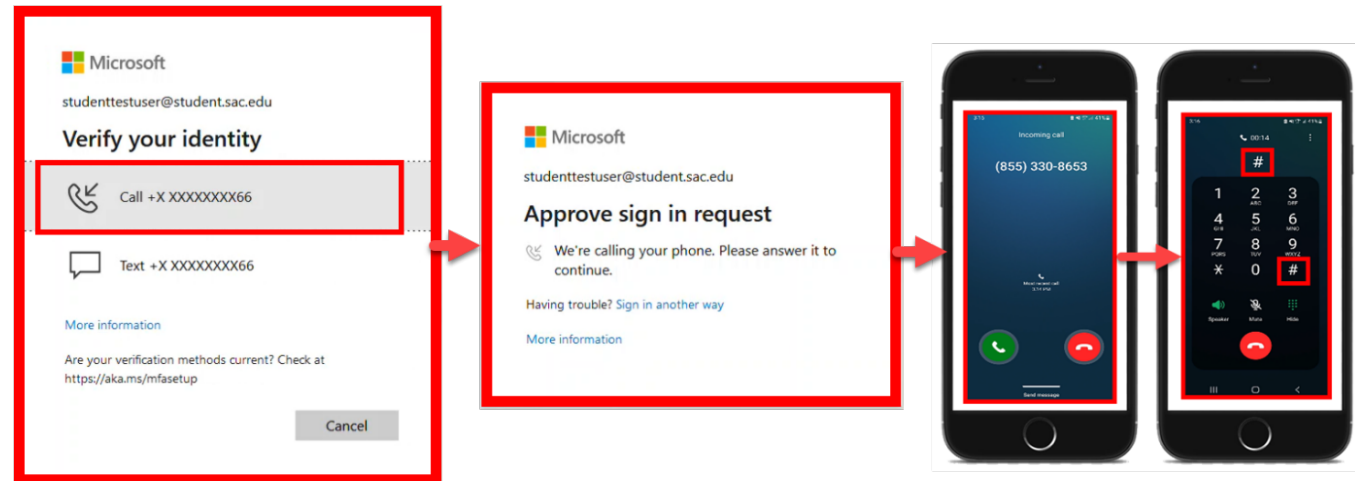
STEP 2 – Select “I want to set up a different method,” then select Phone.

STEP 3 – Enter phone number, then select “Call Me”.

STEP 4 – Answer the phone call from Microsoft and press # key to verify.

STEP 5 – Complete setup and Office.com login.

STEP 6 – Verify your identity with Phone call on next login.





Hardware Token

STEP 1 – Request a Hardware Token from the ITS Department.

STEP 2 – Login to Office.com with your Single Sign-on (SSO) Username.

STEP 3 – Enter the Verification Code.

STEP 4 – Complete Office.com login.

STEP 5 – Verify your identity with Hardware Token on next login.



Contact ITS Help Desk at
helpdesk@rsccd.edu or 714-564-4357 Ext 0
to request a Hardware Token.



Hardware Token

STEP 1 – Request a Hardware Token from the ITS Department.

STEP 2 – Login to Office.com with your Single Sign-on (SSO) Username.

STEP 3 – Enter the Verification Code.

STEP 4 – Complete Office.com login.

STEP 5 – Verify your identity with Hardware Token on next login.

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

Santa Ana 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@rscdd.edu
Example: Smith_John@rscdd.edu



Hardware Token

STEP 1 – Request a Hardware Token from the ITS Department.

STEP 2 – Login to Office.com with your Single Sign-on (SSO) Username.

STEP 3 – Enter the Verification Code.

STEP 4 – Complete Office.com login.

STEP 5 – Verify your identity with Hardware Token on next login.



Microsoft
studenttestuser@student.sac.edu

Enter code

Enter the code displayed on your authentication token

658896

[More information](#)

Verify



Hardware Token

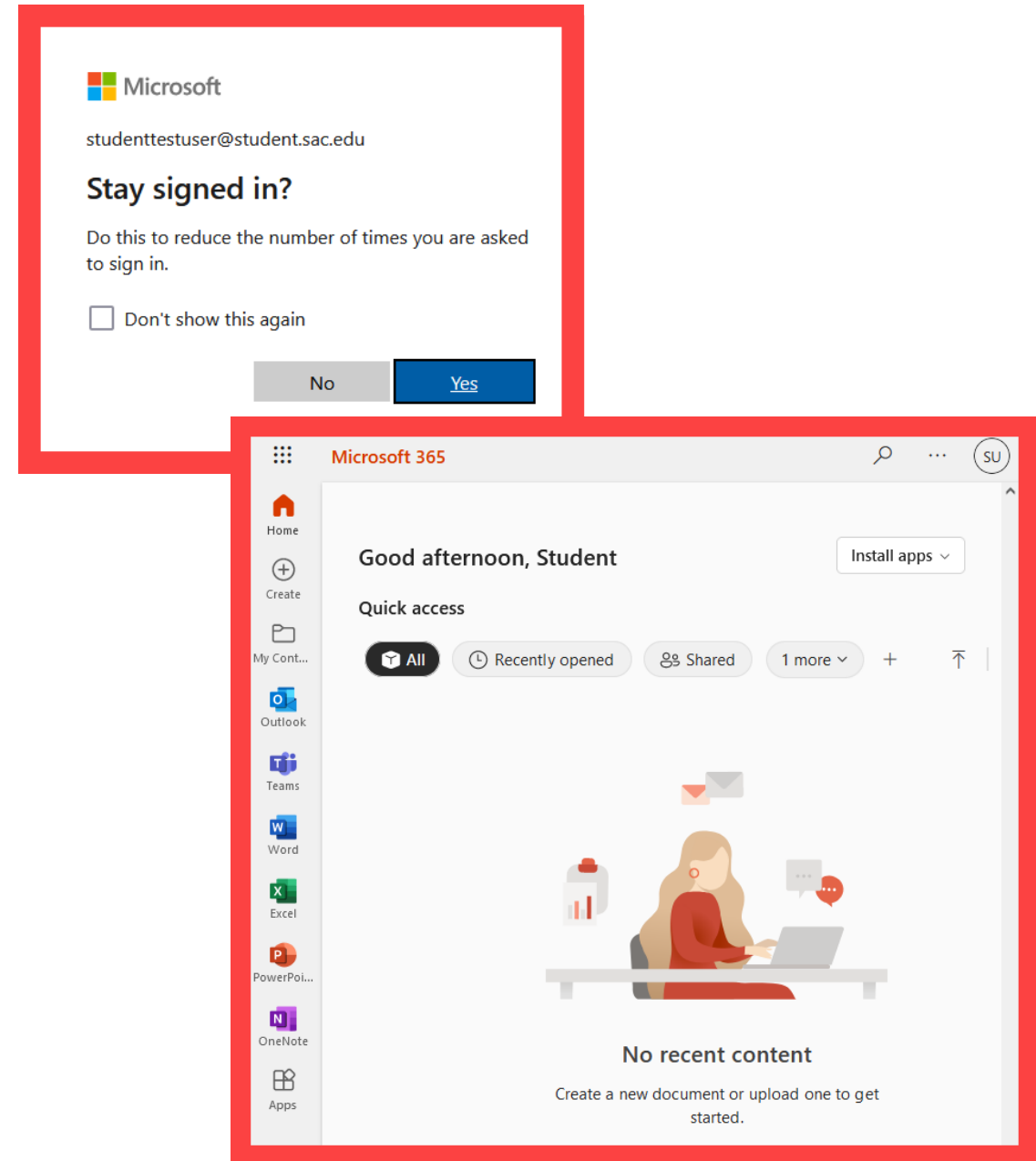
STEP 1 – Request a Hardware Token from the ITS Department.

STEP 2 – Login to Office.com with your Single Sign-on (SSO) Username.

STEP 3 – Enter the Verification Code.

STEP 4 – Complete Office.com login.

STEP 5 – Verify your identity with Hardware Token on next login.





Hardware Token

STEP 1 – Request a Hardware Token from the ITS Department.

STEP 2 – Login to Office.com with your Single Sign-on (SSO) Username.

STEP 3 – Enter the Verification Code.

STEP 4 – Complete Office.com login.

STEP 5 – Verify your identity with Hardware Token on next login.

A screenshot of the Microsoft Office.com login interface. At the top is the Microsoft logo and the email address 'studenttestuser@student.sac.edu'. Below this is the heading 'Enter code'. A sub-instruction says 'Enter the code displayed on your authentication token'. A text input field contains the number '658896'. Below the input field is a link for 'More information'. At the bottom right is a blue 'Verify' button. Numbered callouts are present: a red box labeled '2' around the input field, and a yellow box labeled '3' around the 'Verify' button.



ITS strongly recommends setting up at least 2 different MFA Methods.

(If you lose access to one method, you can still sign in with the other.)

Example:

Primary method: **Authenticator app**



Backup method: **Hardware Token**



Manage Your Backup Authentication Methods

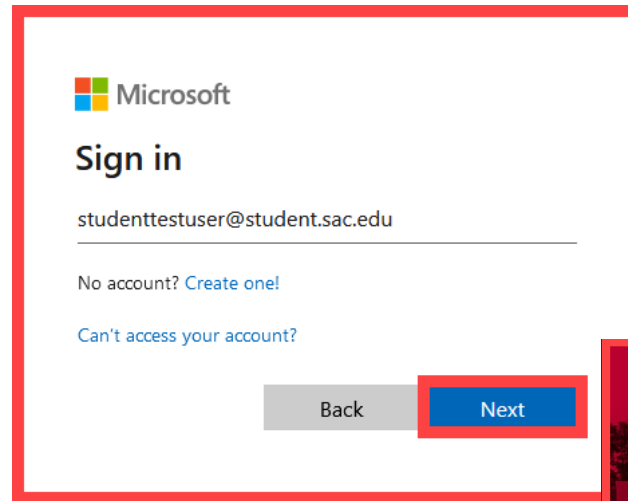
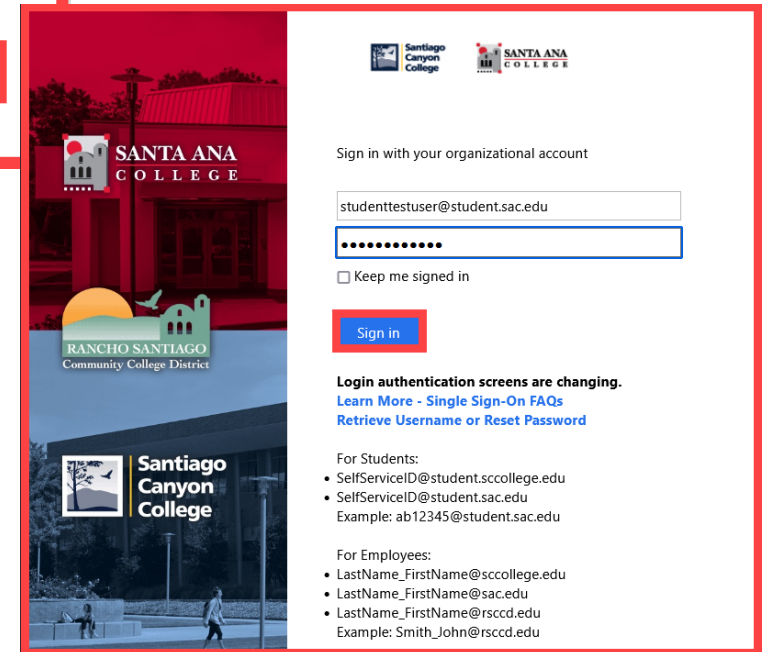
STEP 1 – Sign into Office.com

STEP 2 – Navigate to My Account page from Microsoft 365 Home Page

STEP 3 – On My Account page, under Security Info, select Update Info

STEP 4 – Add, Delete, or Change Your Sign-In Methods

NOTE: Go to <https://aka.ms/mfasetup> for the direct link to manage your MFA sign-in methods.

A screenshot of the Microsoft sign-in page. It features the Microsoft logo at the top left. Below it, the text "Sign in" is displayed. A text input field contains the email address "studenttestuser@student.sac.edu". Below the input field, there are two links: "No account? Create one!" and "Can't access your account?". At the bottom right, there are two buttons: a grey "Back" button and a blue "Next" button. The "Next" button is highlighted with a red border.A screenshot of the Santiago Canyon College login page. The page has a red header with the college's logo and name. Below the header, there is a section for "Sign in with your organizational account". It includes a text input field for the email address "studenttestuser@student.sac.edu" and a password input field with masked characters. Below the password field, there is a checkbox labeled "Keep me signed in". A blue "Sign in" button is located below the checkbox. To the left of the login form, there is a vertical banner with images of the college campus and the text "SANTA ANA COLLEGE" and "RANCHO SANTIAGO Community College District". Below the login form, there is a section titled "Login authentication screens are changing." with links to "Learn More - Single Sign-On FAQs" and "Retrieve Username or Reset Password". At the bottom, there are two sections: "For Students:" with email addresses "SelfServiceID@student.sccollege.edu", "SelfServiceID@student.sac.edu", and an example "ab12345@student.sac.edu"; and "For Employees:" with email addresses "LastName_FirstName@sccollege.edu", "LastName_FirstName@sac.edu", and "LastName_FirstName@rscdd.edu", with an example "Smith_John@rscdd.edu".

Manage Your Backup Authentication Methods

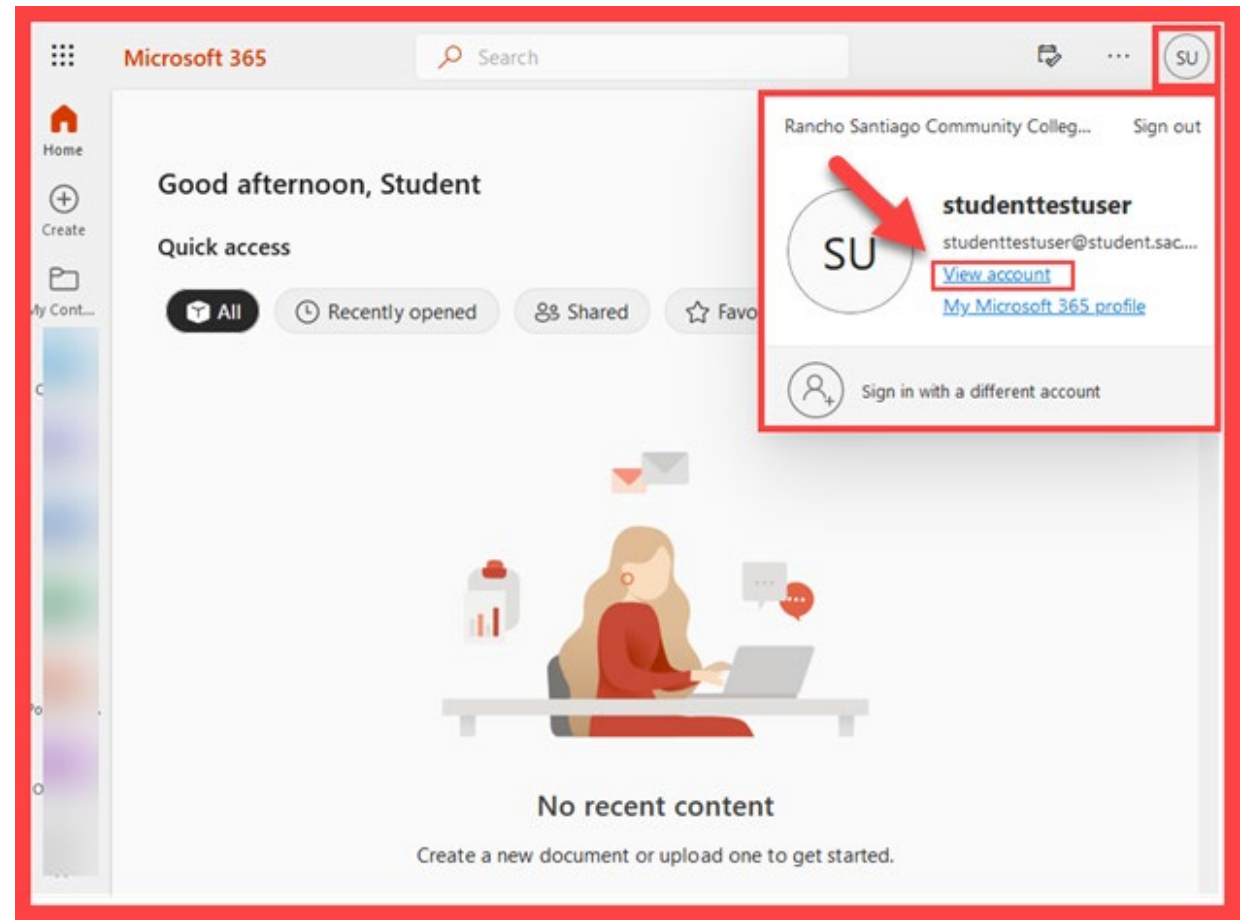
STEP 1 – Sign into Office.com

STEP 2 – Navigate to My Account page from Microsoft 365 Home Page

STEP 3 – On My Account page, under Security Info, select Update Info

STEP 4 – Add, Delete, or Change Your Sign-In Methods

NOTE: Go to <https://aka.ms/mfasetup> for the direct link to manage your MFA sign-in methods.



Manage Your Backup Authentication Methods

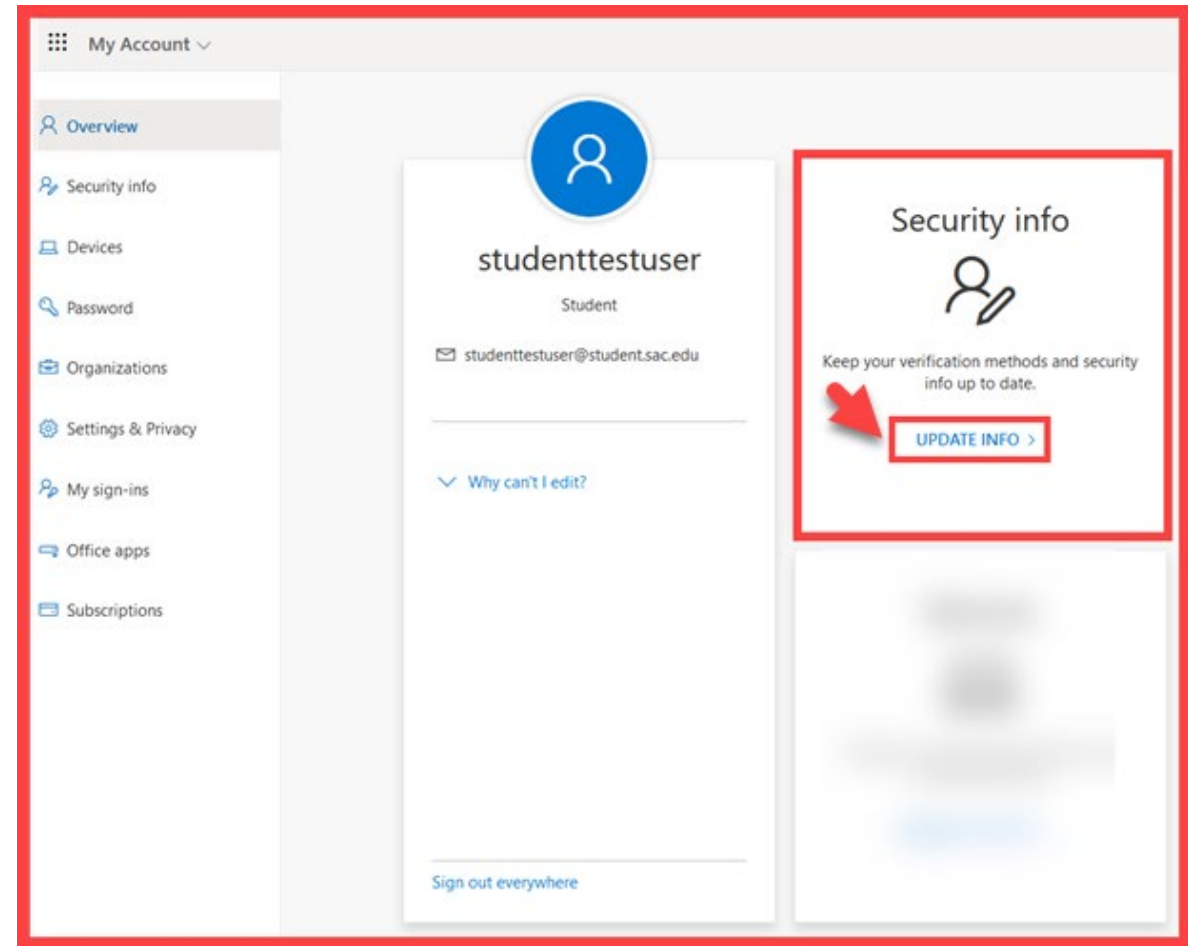
STEP 1 – Sign into Office.com

STEP 2 – Navigate to My Account page from Microsoft 365 Home Page

STEP 3 – On My Account page, under Security Info, select Update Info

STEP 4 – Add, Delete, or Change Your Sign-In Methods

NOTE: Go to <https://aka.ms/mfasetup> for the direct link to manage your MFA sign-in methods.



Manage Your Backup Authentication Methods

STEP 1 – Sign into Office.com

STEP 2 – Navigate to My Account page from Microsoft 365 Home Page

STEP 3 – On My Account page, under Security Info, select Update Info

STEP 4 – Add, Delete, or Change Your Sign-In Methods

NOTE: Go to <https://aka.ms/mfasetup> for the direct link to manage your MFA sign-in methods.

