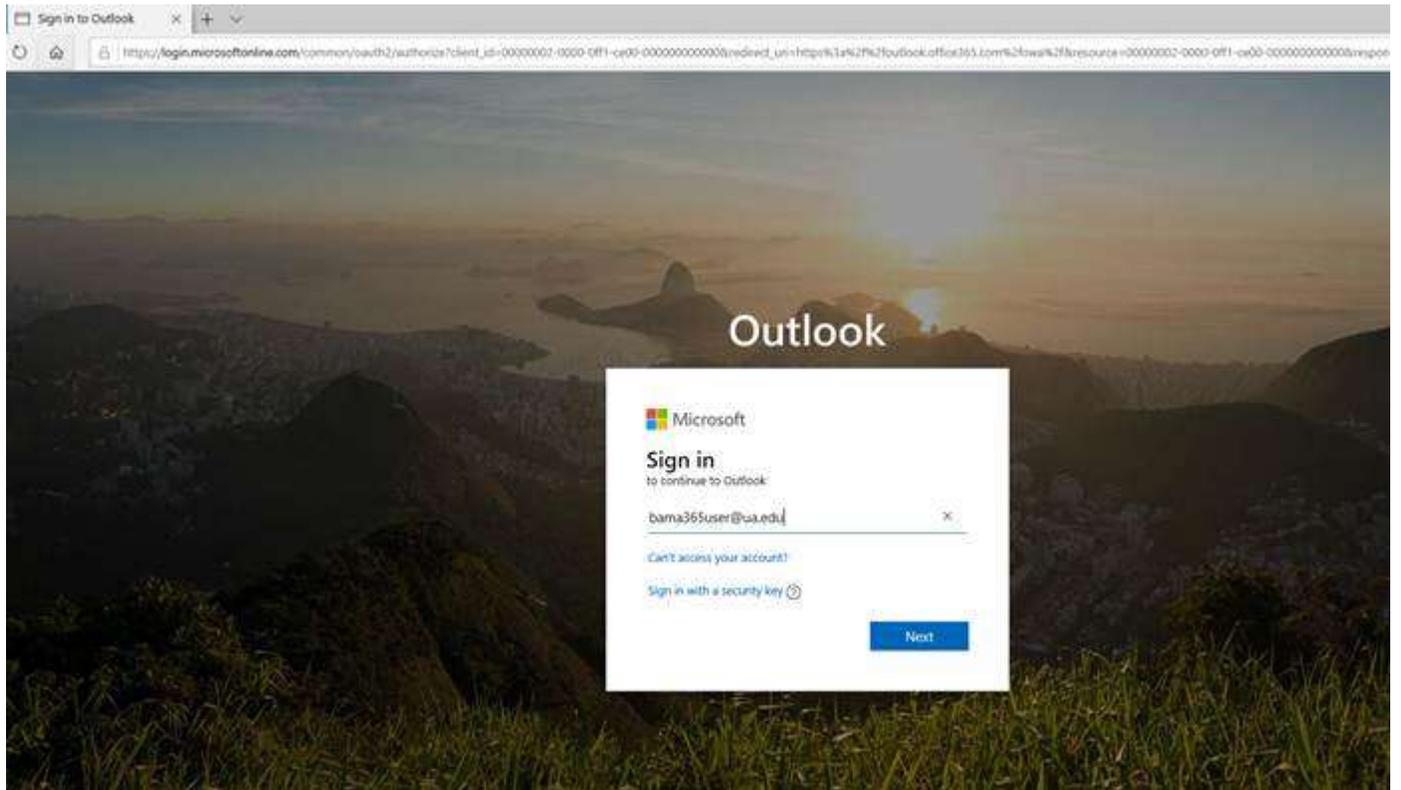


Microsoft Multi-Factor Authentication for Retired Users

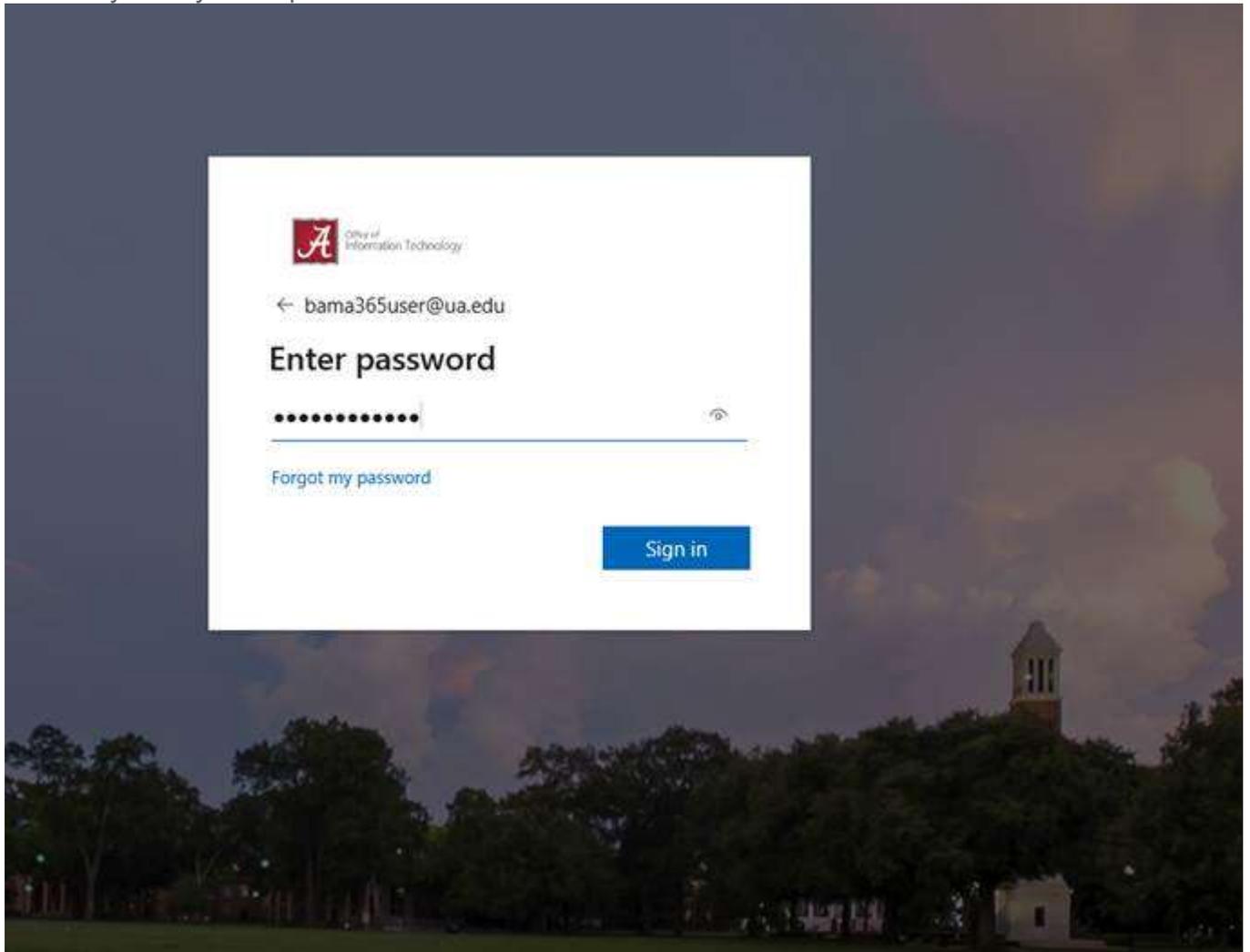
To protect UA email accounts from cyber criminals, multi-factor authentication is required. For active students, faculty and staff, Duo is the required method. For retirees, Microsoft multi-factor is the required method. Learn more about [Microsoft multi-factor authentication](#).

Activate Microsoft Multi-Factor Authentication

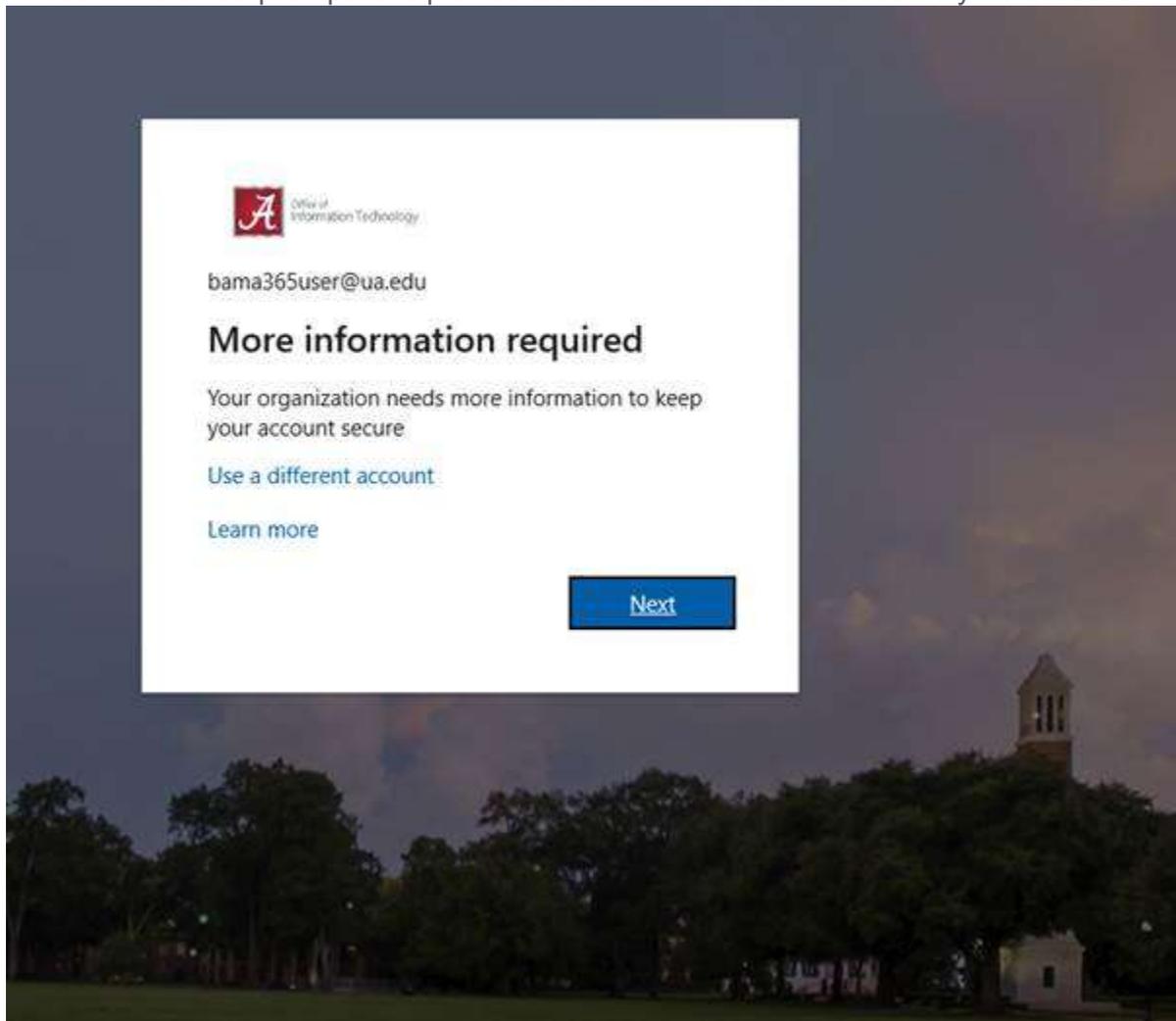
1. Visit outlook.office365.com and login with your myBamausername@ua.edu email address.



2. Enter your myBama password.



3. You will then be prompted to provide additional information to secure your account.



4. Select “Authentication Phone” and “United States” then enter your phone number.

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Authentication phone

United States (+1) 2053485377

Method

Send me a code by text message

Call me

Next

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

©2020 Microsoft | Legal | Privacy

5. The system will call you, and ask you to press # to confirm that you have requested the authentication.

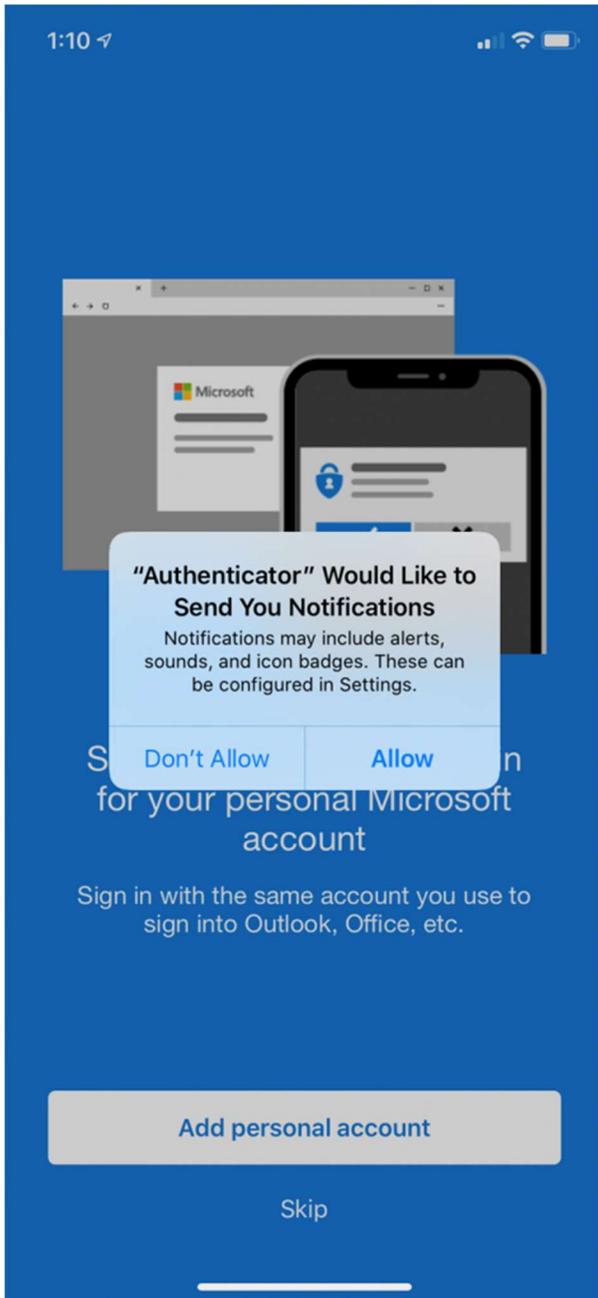
6. Click “done” to complete the registration.

Additional Authentication Options

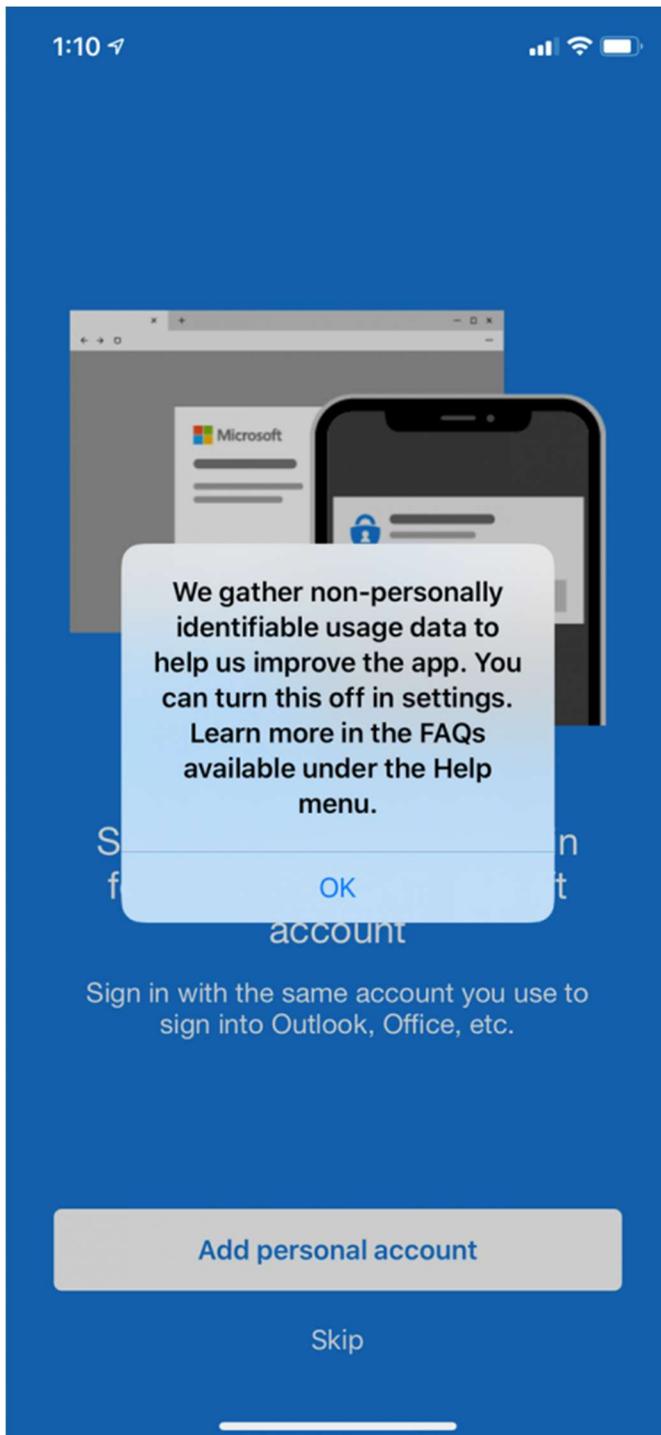
If you would like to set up additional authentication options, such as the Microsoft 2 Factor Authentication app, visit <https://aka.ms/mfasetup> on a computer or device other than your mobile phone. To set up the authenticator app, check the “Authentication app or Token” checkbox, then click the “Set up Authenticator app” button.

The screenshot shows the 'Additional security verification' settings page for a Microsoft account. The page title is 'Additional security verification App Passwords'. A header bar includes the Office of Information Technology logo on the left and the user email 'bama365user@ua.edu' with a help icon on the right. The main heading is 'Additional security verification App Passwords'. Below this, a paragraph explains that signing in with a password also requires a response from a registered device. A link 'View video to know how to secure your account' is provided. The question 'what's your preferred option?' is followed by a dropdown menu set to 'Use verification code from app or'. A red warning message states: 'Microsoft Authenticator app option must be enabled and configured to select this preferred verification option.' The question 'how would you like to respond?' is followed by the instruction 'Set up one or more of these options. Learn more'. There are four options listed: 'Authentication phone' (checked), 'Office phone' (unchecked), 'Alternate authentication phone' (unchecked), and 'Authenticator app or Token' (checked). The 'Authentication phone' option has a dropdown for 'United States (+1)' and a text input for '2053485377'. The 'Office phone' option has a dropdown for 'Select your country or region' and a text input. The 'Alternate authentication phone' option has a dropdown for 'Select your country or region' and a text input. The 'Authenticator app or Token' option has a blue button labeled 'Set up Authenticator app'. At the bottom, there are 'Save' and 'cancel' buttons. A footer note states: 'Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.' The footer also includes '©2020 Microsoft Legal | Privacy'.

Visit the app store on your mobile device and download and install the “Microsoft Authenticator” app. Once installed, open the application on your mobile device. If prompted, allow the device to send notifications.

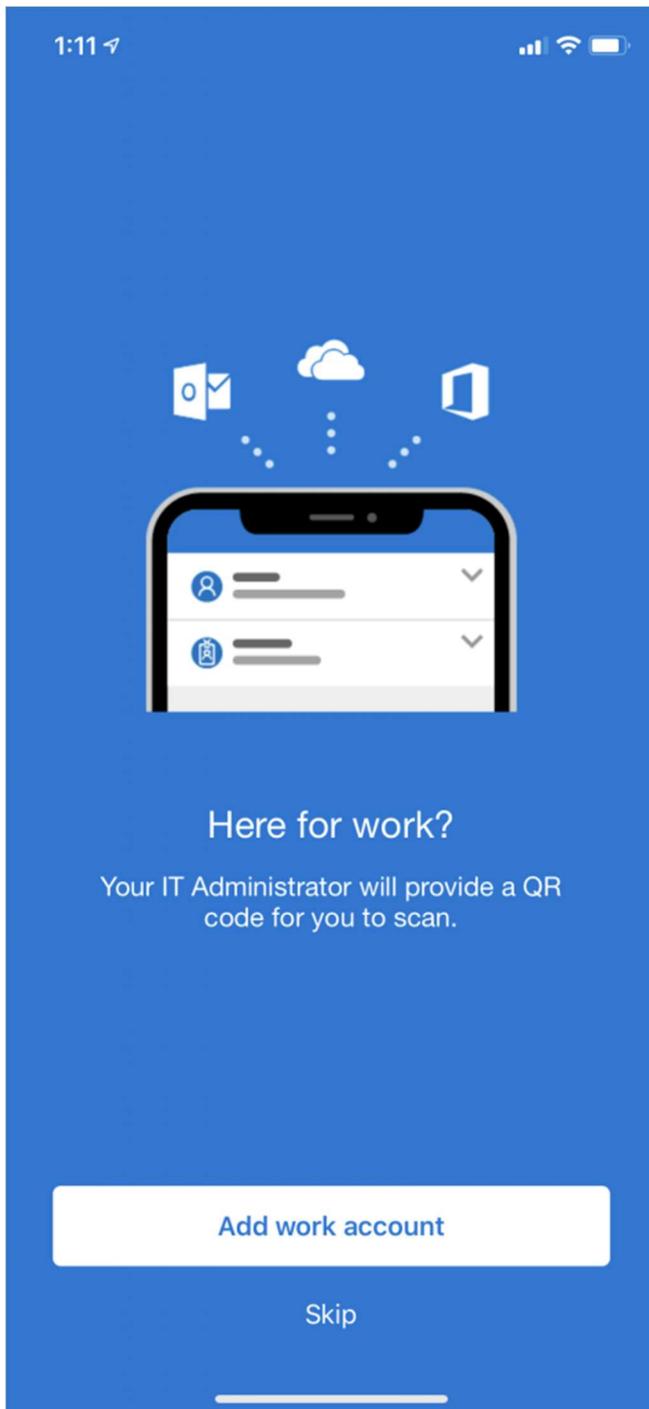


Tap OK to acknowledge the privacy settings



Skip the first step for setting up a personal account, and the second step for adding external accounts.

On the third step, tap the “Add work account” button.



Allow the authenticator app to access your camera, and then scan the QR code back on the web page

1:12



Accounts



Ready to add your first account?



**"Authenticator" Would Like to
Access the Camera**

May be needed to scan QR code to
add a new account

Don't Allow

OK

Add account

Already have a backup?
Sign in to your recovery account.

Begin recovery

e from app or  Microsoft Authenticator app option must be enabled and configured to select this preferred verification option.

Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for [Windows Phone](#), [Android](#) or [iOS](#).
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.



[Configure app without notifications](#)

If you are unable to scan the image, enter the following information in your app.
Code: 895 536 759
Url: <https://cys01napad11.na.phonefactor.net/pad/005783753>

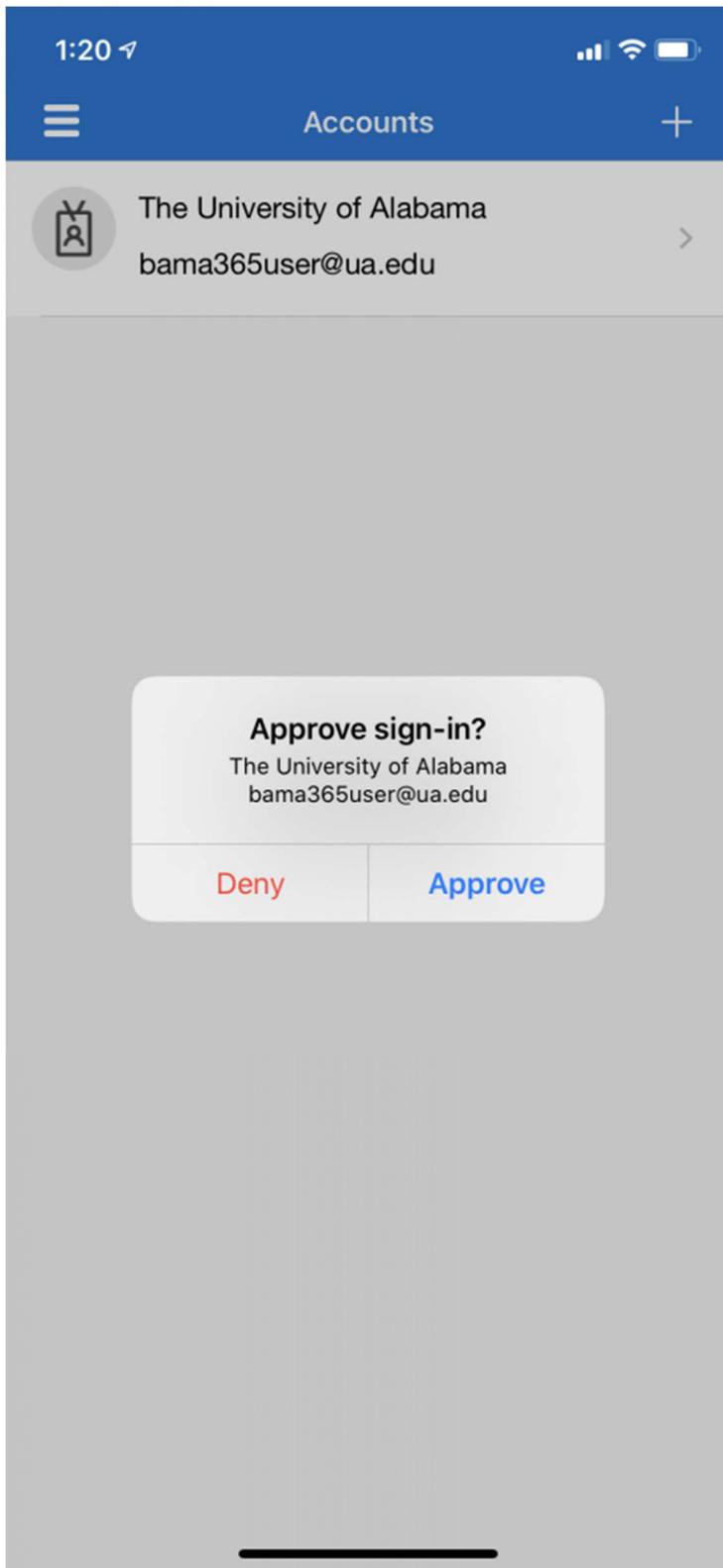
If the app displays a six-digit code, choose "Next".

[Next](#) [cancel](#)

An entry for "The University of Alabama" will appear in the app

On the web page on the first device, click "next"

Click "Approve sign-in" on the mobile device



On the web page, you can then select your default notification and click Save

Additional security verification App Passwords

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password. [View video to know how to secure your account](#)

what's your preferred option?

We'll use this verification option by default.

Notify me through app

how would you like to respond?

Set up one or more of these options. [Learn more](#)

<input checked="" type="checkbox"/> Authentication phone	United States (+1)	2053485377
<input type="checkbox"/> Office phone	Select your country or region	Extension
<input type="checkbox"/> Alternate authentication phone	Select your country or region	

Authenticator app or Token [Set up Authenticator app](#)

Authenticator app - Michael's iPhone [Delete](#)

[Save](#) [cancel](#)

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

If after following the above steps, you have any issues, please contact the OIT Helpdesk at (205) 348-5555.