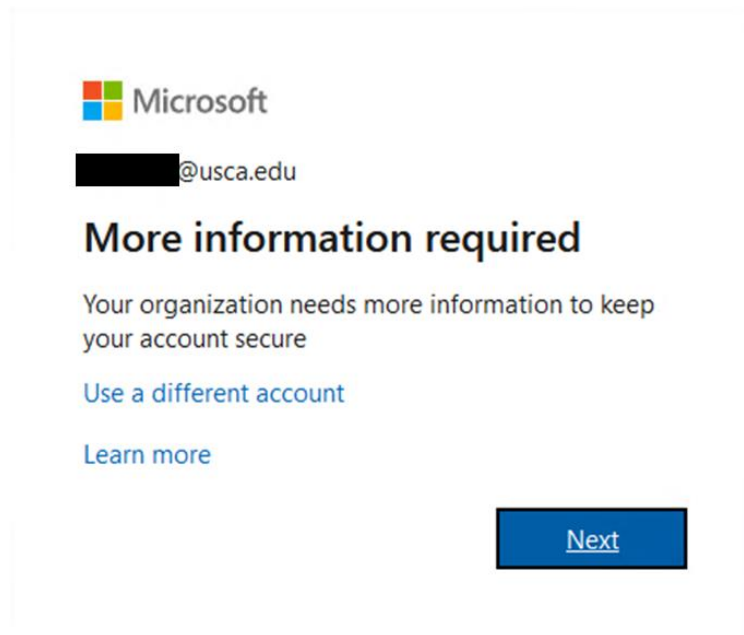


## **UofSC Aiken – Computer Services Division** **Multifactor Authentication (MFA) Setup Procedure**

Once a usca.edu account has been enabled for MFA, you will be prompted to complete the MFA setup process upon their next account login. You will be presented with the following dialog after logging into <https://portal.office.edu/>:



After selecting Next, the next page will prompt you to enter a phone number and select the authentication method: text message or phone call. A valid phone number should be entered, and the desired authentication method selected:

## 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)

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.

After selecting Next, you will receive a phone call or text message at the provided phone number and given a six-digit code. That code should be entered on the next verification page:

## Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

### Step 2: We've sent a text message to your phone at [REDACTED]

When you receive the verification code, enter it here

Cancel

Verify

Upon successful verification, MFA will be enabled and required on your account. You will then be presented with a page informing them about using certain applications. Outlook, Apple Mail, the Office suite, and others are incompatible with MFA by phone. There are two methods for using these applications with MFA. The first is presented on the following page:

## Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

### Step 3: Keep using your existing applications

In some apps, like Outlook, Apple Mail, and Microsoft Office, you can't use a phone to secure your account. To use these apps, you'll need to create a new "app password" to use in place of your work or school account password.

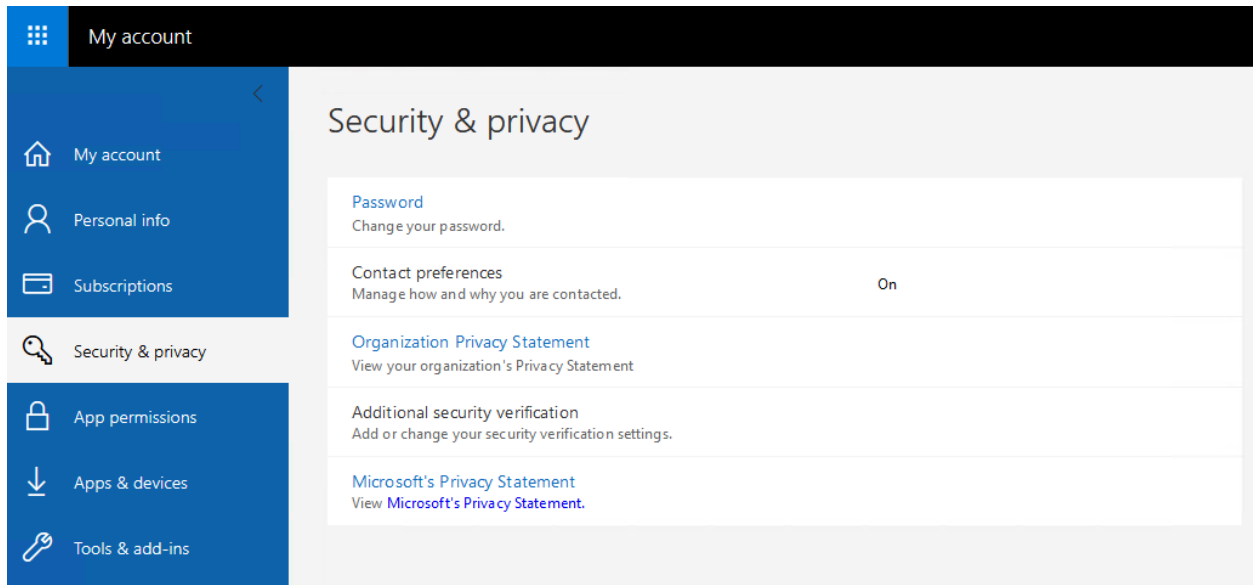
To create an app password, go to:

<https://aka.ms/CreateAppPassword>

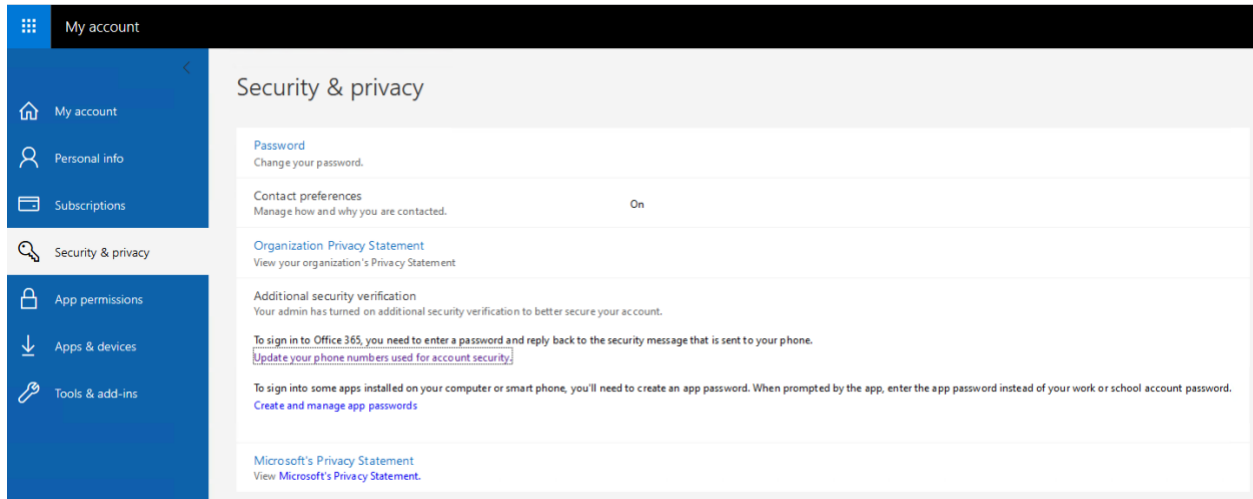
Done

You can create app passwords by going to: <https://aka.ms/CreateAppPassword>.

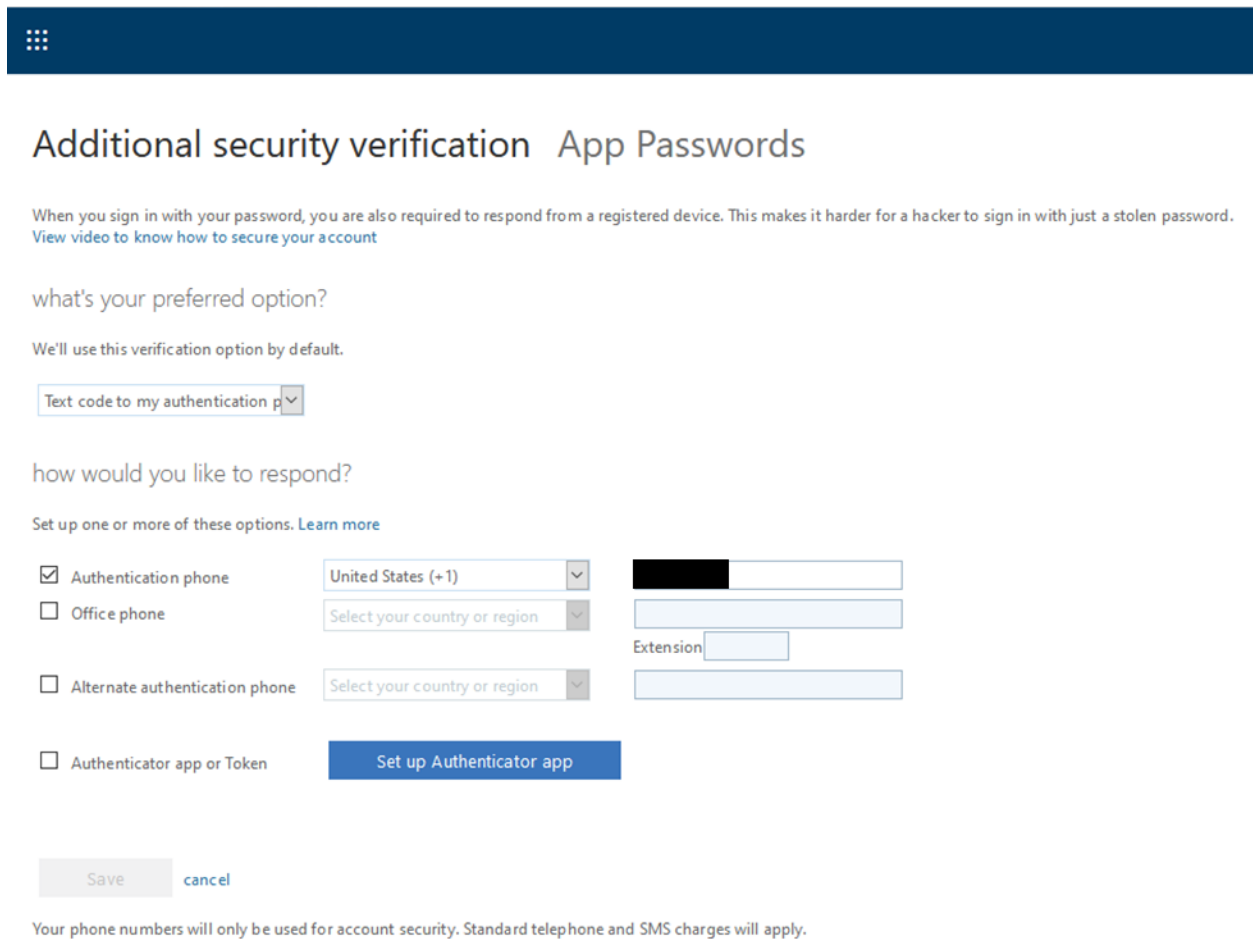
The second method is to setup MFA with the Microsoft Authenticator App. This method uses your cell phone and the Microsoft Authenticator app which is available in both the Apple and Google app store. After selecting Done, select the account avatar at the top right of the browser and then select View Account. Once the account page has loaded, select Security & Privacy on the left:



In the Security & Privacy menu, select Additional Security Verification:

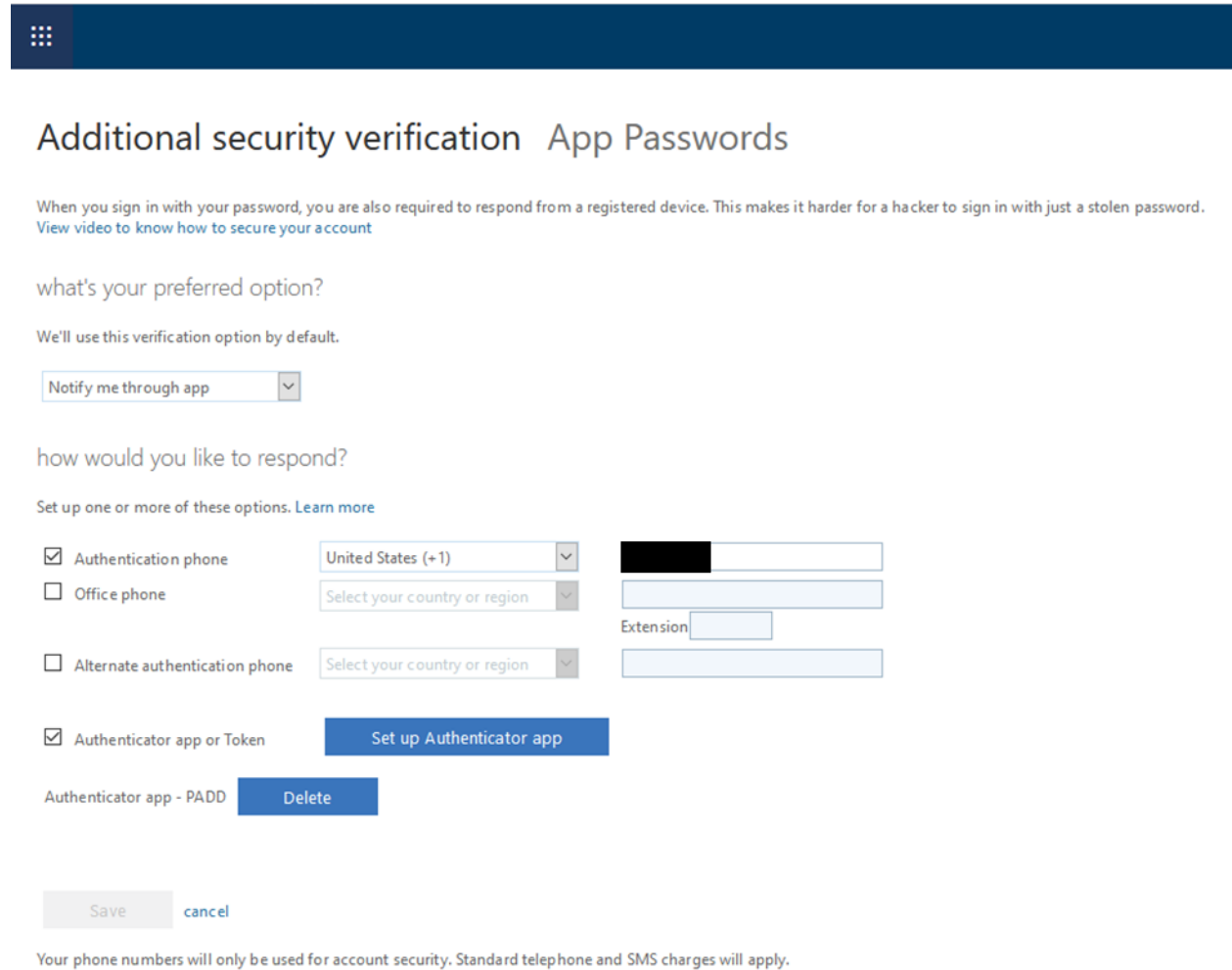


Then select Update Your Phone Numbers Used for Account Security to get to this page:



Additional phone numbers can be setup on this page; however, to setup the Microsoft Authenticator App, first select the Set Up Authenticator App button. A page with a QR code will appear.

Launch the Microsoft Authenticator App and select the + symbol at the top right. When the QR scanner is visible, point the phone's camera to the QR code displayed in the browser. Upon a successful scan, the Authenticator app will create a new entry for the usca.edu account. Also, in the browser, the following page will be displayed:



The screenshot shows a dark blue header with a white grid icon. Below it, the page title is "Additional security verification App Passwords". A sub-header reads: "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](#)".

The main content area asks "what's your preferred option?" and states "We'll use this verification option by default." Below this is a dropdown menu with "Notify me through app" selected.

Next, it asks "how would you like to respond?" and says "Set up one or more of these options. [Learn more](#)".

There are three phone-related options, each with a checkbox and a country/region dropdown:

- Authentication phone: Country dropdown is "United States (+1)". A blacked-out phone number is visible in the input field.
- Office phone: Country dropdown is "Select your country or region".
- Alternate authentication phone: Country dropdown is "Select your country or region".

Each phone option has an "Extension" input field.

The "Authenticator app or Token" option is checked. Below it is a blue button labeled "Set up Authenticator app".

Below that, there is an entry for "Authenticator app - PADD" with a blue "Delete" button next to it.

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 box next to the Authenticator App or Token text should be checked and a new Authenticator App entry should be visible below it. Once this is visible, you have successfully setup MFA on their account with the Authenticator app. You can close their browser and navigate away from this page.