Setup Guide for Multi-Factor Authentication (MFA)

All Lipscomb accounts must set up Multi-Factor-Authentication (MFA) in order to login to any part of your account. These instructions will walk you through selecting the best option for you to reset your preferred method. *This guide is useful when you are setting up your account for the first time or when IT has reset/refreshed your account and removed an old/former method that you had setup.*

What is Multi-Factor Authentication?

Multi-factor authentication is a second authentication that comes after your password (your 'first' authentication). This second factor sends a code or a request that must be verified to allow you to continue signing in. This means that if someone steals your password, they then need to also get past the second step. This helps keep your account secure.

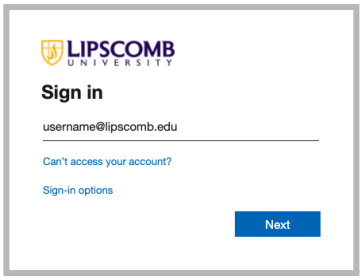
Methods to Choose From:

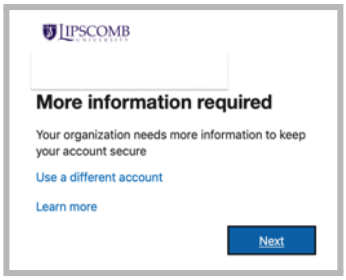
- Authenticator Apps (Microsoft, Google, Duo, or LastPass)
- SMS text message to a mobile phone
- Voice call to a phone

If you will be traveling internationally outside the USA, ensure that you have at least one Authenticator App setup for each wifi-capable smart device you will be taking with you. Do not rely on a text message for international travel.*

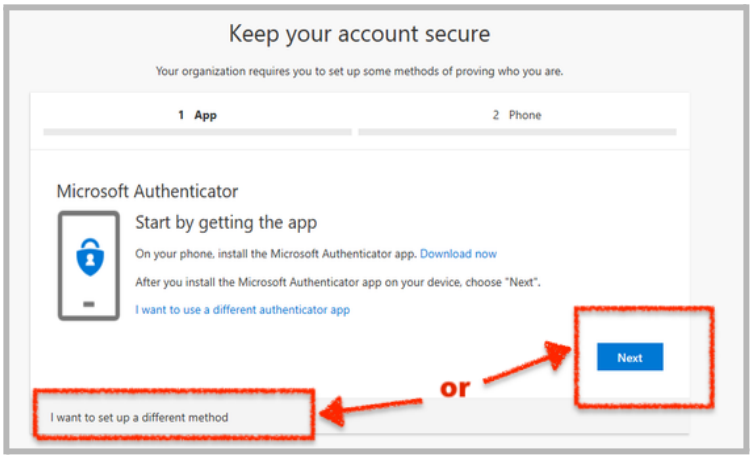
Step 1: How do I set it up?

- ☐ Go to the my.Lipscomb Portal my.lipscomb.edu where you will be prompted to sign in. Enter your Lipscomb email address and password. When prompted with the "More Information Required" screen, click Next.





The Microsoft Authenticator App will be the default option. Go to the appropriate section guides on each method to setup your preferred primary and back-up options.



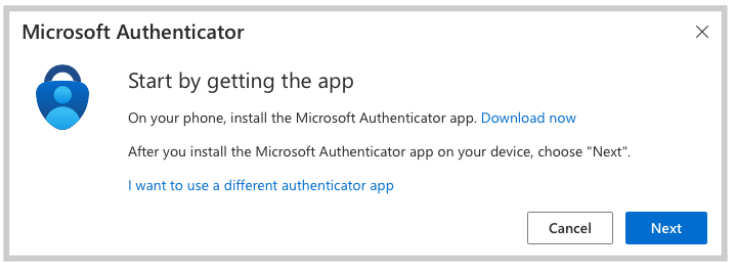
Choice 1: Microsoft Authenticator App Setup

The process to setup the Microsoft Authenticator app can be done just using your mobile device ***or*** using a computer + mobile device. Each set of instructions are slightly different and detailed below:

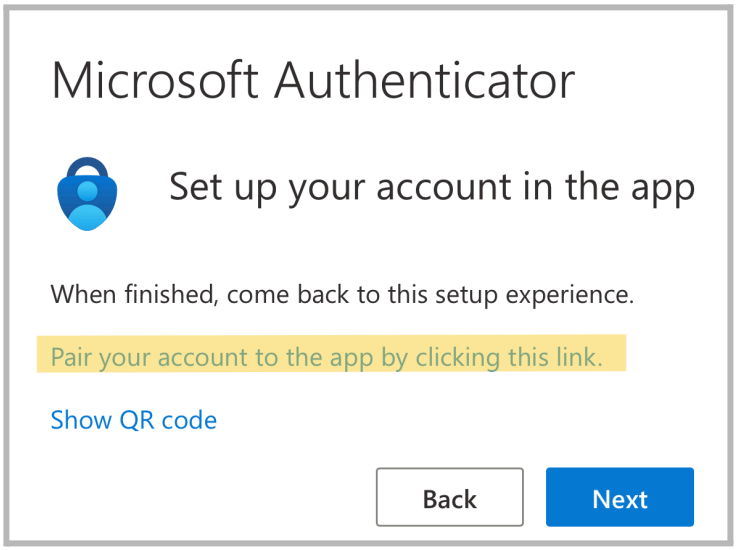
Note: *The Authenticator app is tied to your physical mobile device. If you get a new phone, you'll need to set up a new authenticator app before you disable your old device.*

On a mobile device (only):

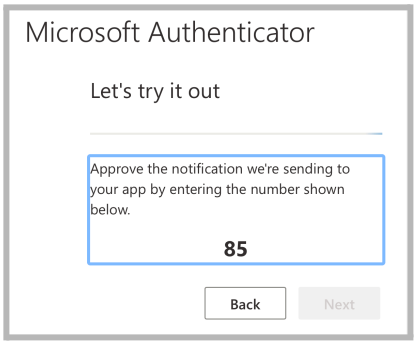
- ☐ Download the Microsoft Authenticator app from your phone's App Store before proceeding. *(*Please Note*: There are 'fake' authenticator apps. Be sure to check you are getting the "Microsoft" one that matches the logo above.)*
- ☐ Do Nothing with the newly downloaded app at this time
- ☐ Open a browser on your mobile device, such as Safari or Chrome. Go to the my.Lipscomb Portal at my.lipscomb.edu and sign in using your Lipscomb email and password
- ☐ You should see "More Information Required" as shown above, click Next.
- ☐ You should next see the "Start by getting the App", click Next.



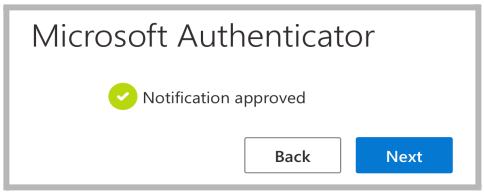
- ☐ You will see this screen. Click on the highlighted link that says "Pair Your account to the app by clicking this link"



- [ ] Click on the highlighted link that says “Pair Your account to the app by clicking this link”
- [ ] It will automatically open the Authenticator app *(You may be asked to open the link in the app. Tap 'Open'.)*
- [ ] Go back in your web browser, tap 'Next'. You will now be asked to test your MFA setup. “Let's try it out” will give you a two-digit number. It will also send you a push notification.



- [ ] Tap the push notification, and enter the two-digit number into Microsoft Authenticator. You will receive an 'Approved' notification if the code has been entered correctly.
- [ ] Go back to the browser and tap next to complete the setup.



- [ ] You have now successfully configured Microsoft Authenticator to secure your account and can continue to use your phone
- [ ] To complete signing in to the my.Lipscomb Portal, you will need to receive a second code from the Authenticator app. Complete the same steps for receiving the code to finish the sign in process.

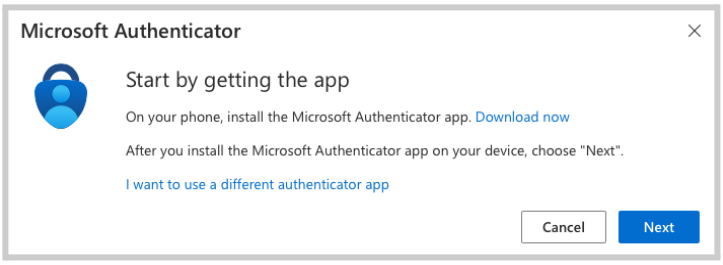
On a computer + mobile device:

- ☐ Download the Microsoft Authenticator app from your phone's App Store before proceeding. *(*Please Note*: There are 'fake' authenticator apps. Be sure to check you are getting the "Microsoft" one that matches the logo above.)

- ☐ Open a browser on your computer, such as Safari or Chrome. Go to the my.Lipscomb Portal at my.lipscomb.edu and sign in using your Lipscomb email and password

- ☐ You should see "More Information Required" as shown above, click Next.

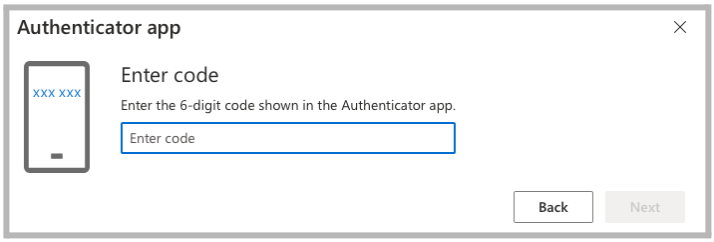
- ☐ You should next see the "Start by getting the App", click Next.



- ☐ Once you've downloaded the app on your smartphone, click on the 'Next' button as seen in the image above. You will be prompted to set up your account on the app on your mobile device.

- ☐ On your mobile device in the Authenticator App, click the + sign in the upper corner and choose Work or school account. You will then be prompted to scan a QR code from your computer or other device's window.

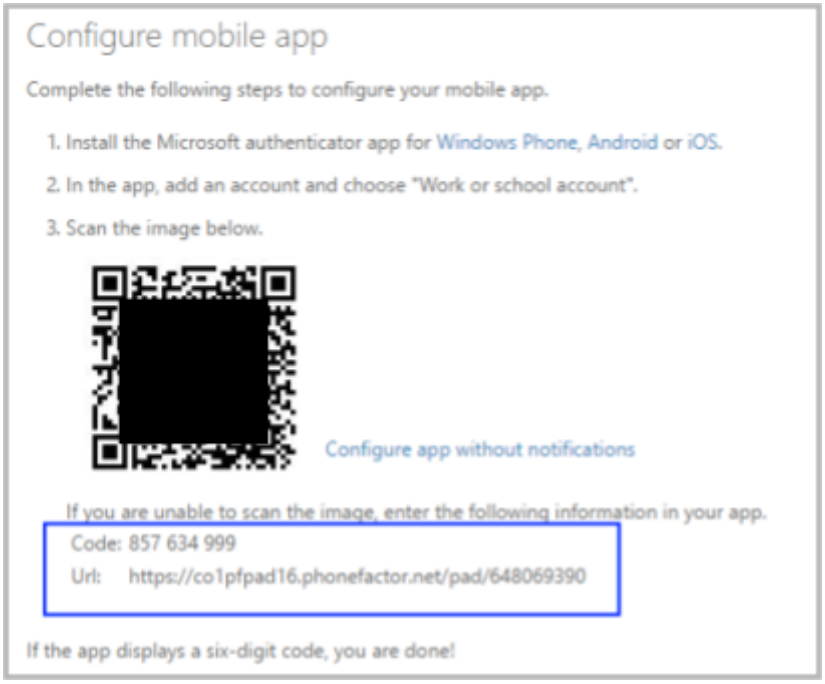
- ☐ You will be prompted to then enter the digits displayed by your app to complete the setup.



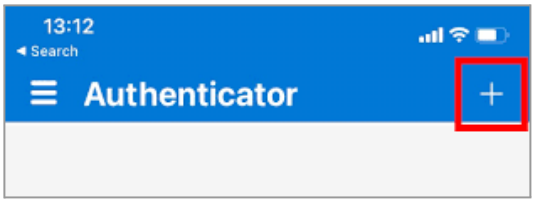
- ☐ Once you've scanned the QR code and clicked Next, it will test the connection with a prompt from the app – click 'Approve'. If the test is successful, you will be logged into your account and have completed the MFA setup.

No QR Code to scan:

- ☐ On your computer, note the **Code and Url** information on the **Configure mobile app** page. Keep this page open so you can see the code and URL.



- ☐ Open the Authenticator app, select **Add account** from the **Customize and control** icon in the upper-right, and then select **Work or School account**.



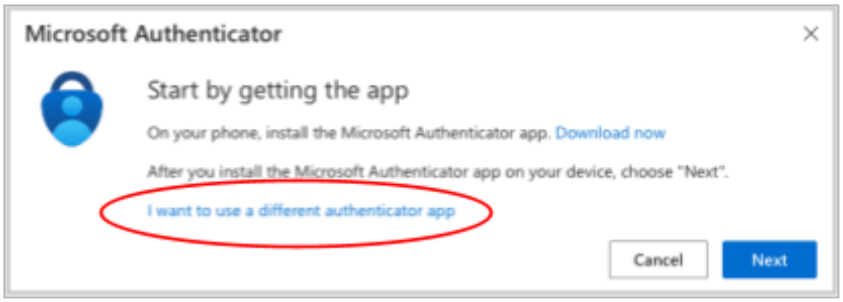
- ☐ Select "**ENTER CODE MANUALLY**".

- ☐ Enter the Code and URL and then select **Finish**.

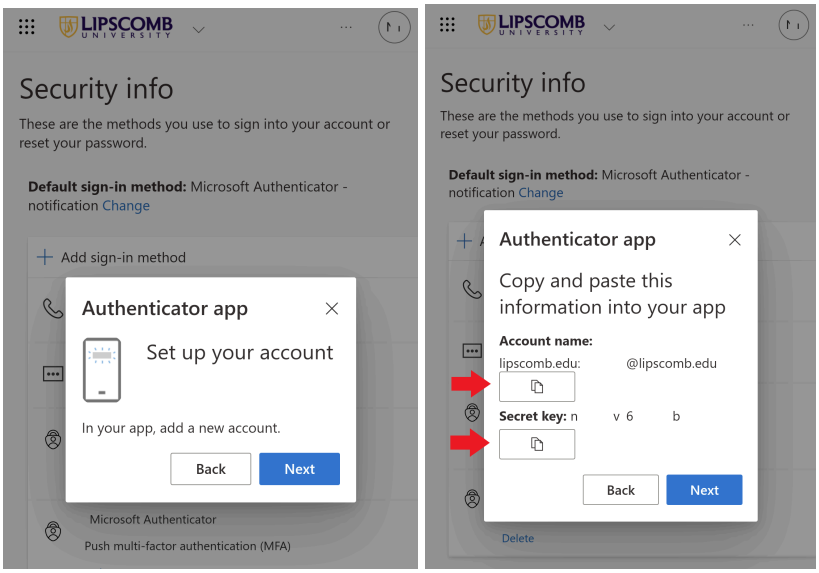
Choice 2: Google Authenticator App Setup

These instructions are for the Google Authenticator app. If you would like to use the Microsoft Authenticator app, please see the previous section.

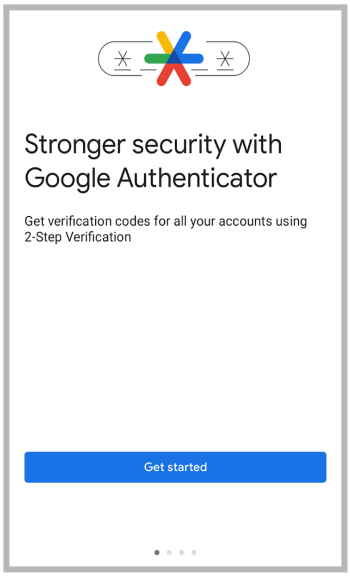
- ☐ Download the Google Authenticator app from your phone's App Store before proceeding.
- ☐ When setting up the app, you should be in the process of accessing the my.Lipscomb Portal for the first time (or after an IT reset), or already logged into your my.Lipscomb account.
- ☐ When you are prompted during the sign-in process for the my.Lipscomb Portal, click on "I want to use a different authenticator app" (see screenshot).

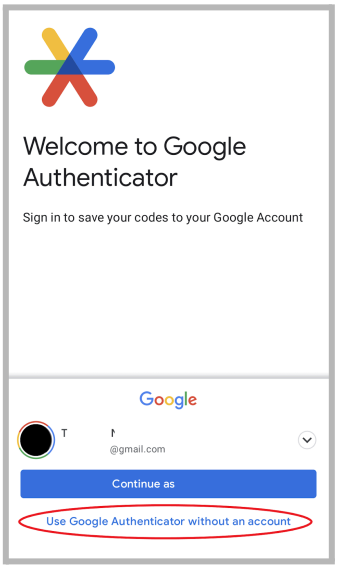


- ☐ After you select "...use a different app", I will ask you to 'setup your account'. Click Next. On the following screen, you will have 2 items: your Account Name and your Secret Key. Keep this screen available, but you will need to change screens here.

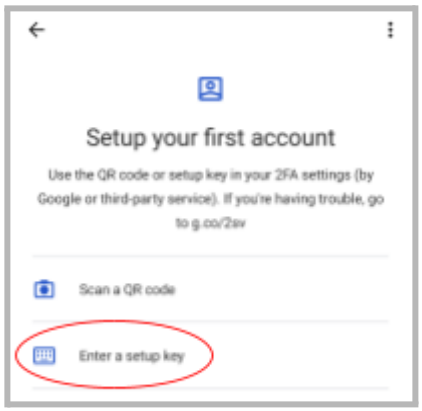


- ☐ Go to your Google Authenticator app that you've downloaded on your smartphone.
- ☐ Click on the "Get Started" button as seen in the image below. You will be prompted to sign in with a Google Account. Instead, ***click on "Use Google Authenticator without an account".***

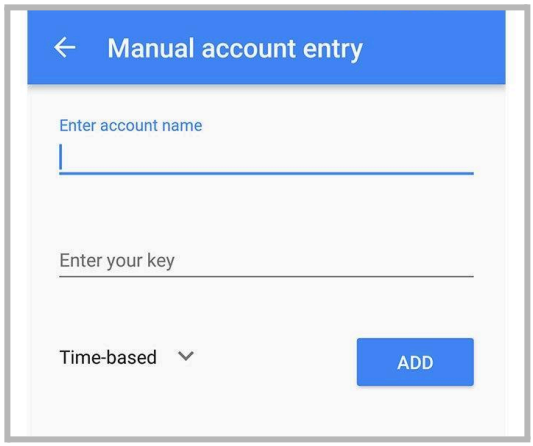




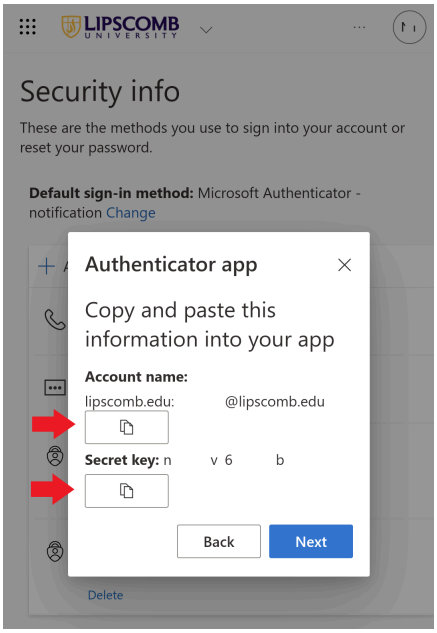
☐ On the next screen, it will ask you to Setup your first account. Click on “Enter a Setup Key”.



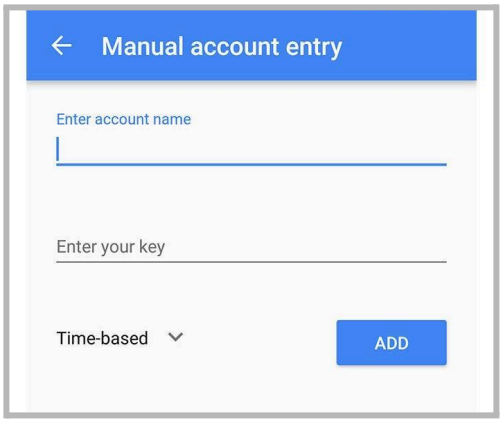
☐ On the next screen, you will be asked to enter an account name and secret key. These were provided to you in an earlier step. You will need to go back & forth between each screen.



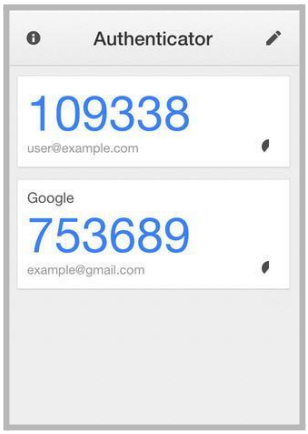
☐ Go back to the my.Lipscomb Portal screen where you had the Account Name and Secret Key available. If you are on the same device, you can click the “Copy” button (red arrow), or you can type it in ***exactly*** as it appears.



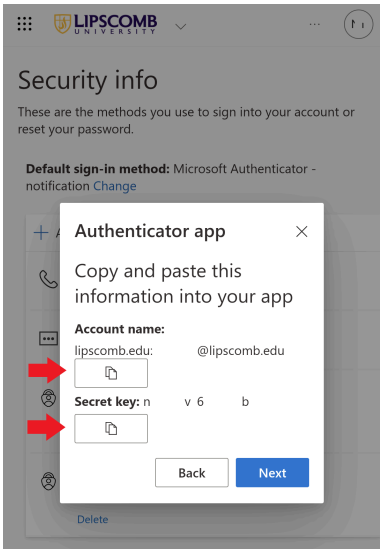
☐ Enter each field, leave the default option for “Time-based” selected, and click “Add”.



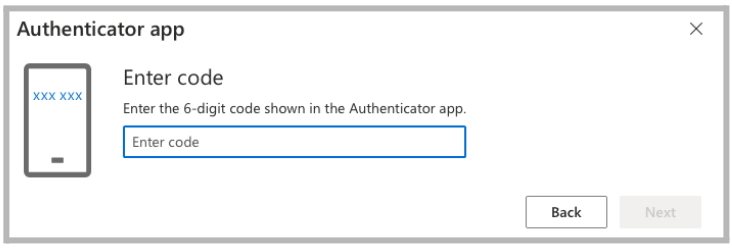
☐ After clicking Add, the Authenticator App will display a 6-digit numeric code. It is time-based, meaning you only have 60 seconds to enter this code. There is a countdown timer on display to show you how long you have left to enter it.



☐ Go back to the my.Lipscomb page that had the Account Name & Secret Key. Click ‘Next’.



☐ On that page, enter the 6-digit numeric code you had from the Google Authenticator.

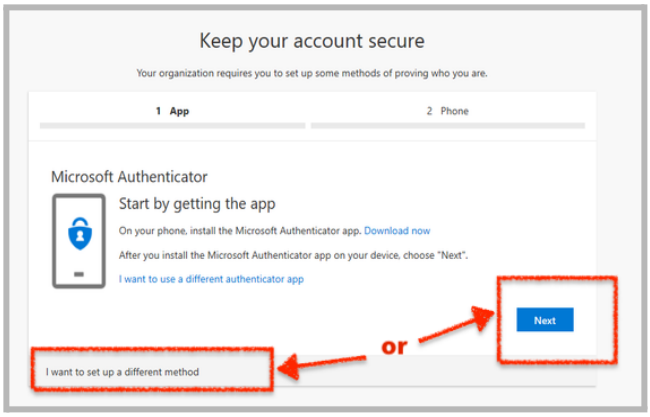


☐ That should complete any setup for using Google.

Choice 3: Text Message/Voice Call Setup

To setup a Text Message / Voice Call:

- ☐ Click the link “I want to set up a different method” at the bottom of the authenticator page.



- ☐ Select Phone from the drop down menu and choose the method you would like to use (voice or text) and then enter your phone number.
  - ☐ If you choose voice, you will be called at the number entered and be prompted to press # to confirm. The caller ID should display the Help Desk phone number 615-966-1777.
  - ☐ If you choose the text message, you will be sent a 6-digit code via text message that you must enter.
- ☐ Follow the prompts until you get a Success! Message.

Choice 4: Alternate Method Setup

You may choose to use a different method, such as a different authenticator app or a hardware key.

- ☐ You may choose to use a different Authenticator App, either Duo Mobile or LastPass Authenticator. Download the App you wish to use to your mobile device. We do not provide instructions for these apps at this time.
- ☐ You can also use a Hardware Authentication Key, such as a YubiKey. Reach out to IT for help with this option.

Step 2: Add Backup MFA Methods

Once you’ve set up your default (or preferred) method, we recommend that you set up at least one alternate method as a backup. This backup method means you will not need to contact IT for a reset. ***This applies for situations like when you get a new phone, you won’t need to contact IT to help you get back into your account.***

The backup methods can be another phone number which can include your office phone number or installation of the authenticator app on another mobile device such as a tablet. For more instructions on how to set up a Backup Method or alter your current methods, please see this document.

If you will be traveling internationally, ensure that you have at least one Authenticator app setup for each wifi-capable smart device you will be taking with you. Do not rely on text method for international travel.

If you need assistance with the setup of your MFA methods, please contact our Help Desk at helpdesk@lipscomb.edu or 615-966-1777 and we will be happy to assist.

.