

Reset Guide for Multi-Factor Authentication (MFA)

This document explains **how to add, update, edit or reset** your authentication methods (phone text, phone call or authenticator app) to all Lipscomb accounts in order to use multi-factor authentication. We require Multi-factor authentication on all Lipscomb accounts as a security measure.

- **These instructions are useful when you still have access to your account and to the my.Lipscomb Portal.** If you do not have access, please see the linked MFA [Setup Guide](#).
- **If you are getting a new phone:** We recommend that you review this guide before you activate a new phone. We recommend that you download the app on your new phone first, get it setup, and then turn in/deactivate your old phone. The app is tied to your device, not your account.
- **If you will be traveling internationally,** ensure that you have at least the Authenticator app setup for each wifi-capable smart device you will be taking. *Do not rely on text messages for international travel.*

What is Multi-Factor Authentication?

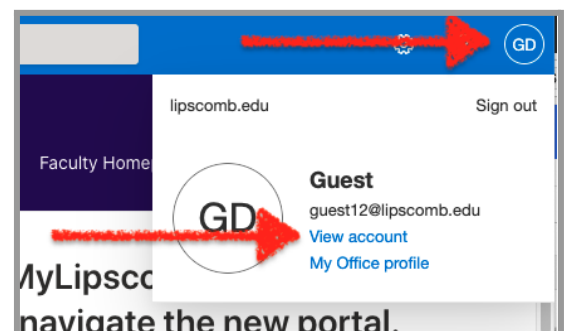
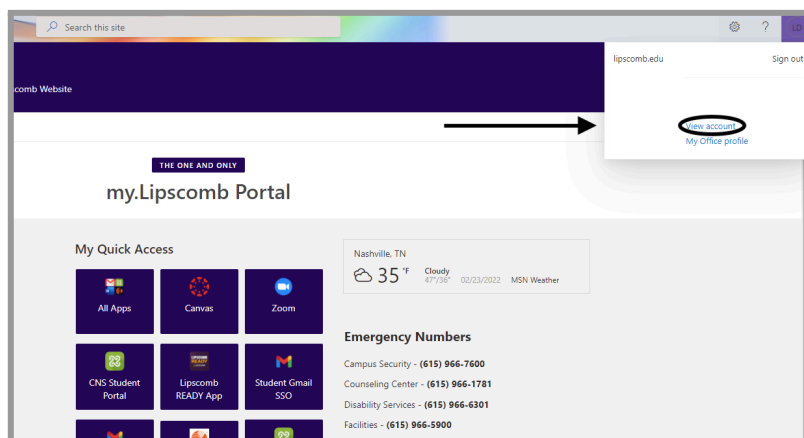
Multi-factor authentication or two-factor authentication is a second authentication that comes after your password (your 'first' authentication). The second authentication sends a code or a request that must be verified to allow you to continue signing in. This means that if someone steals your password,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

Reset Instructions

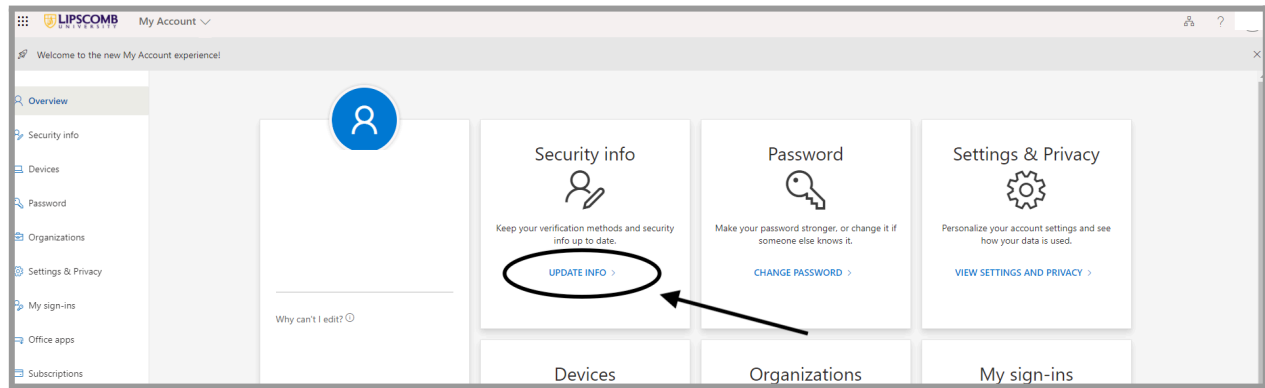
These Reset instructions allow you to edit and/or add an MFA method if you still have access to your my.Lipscomb Portal and your accounts.

[Click Here for Video Instructions](#)

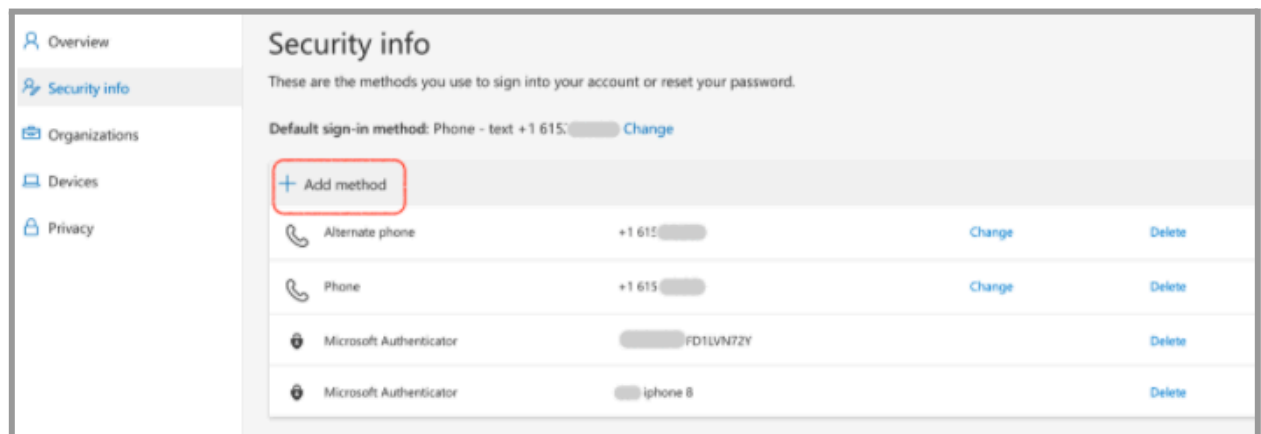
1. Go to my.lipscomb.edu and sign in with your Lipscomb email and password.
2. Once in the site, look for and click on your initials in the circle in the top right corner
3. It will open a small pop-out window. Click "View Account" in that window.



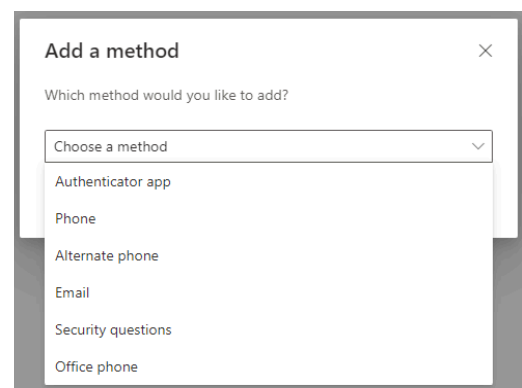
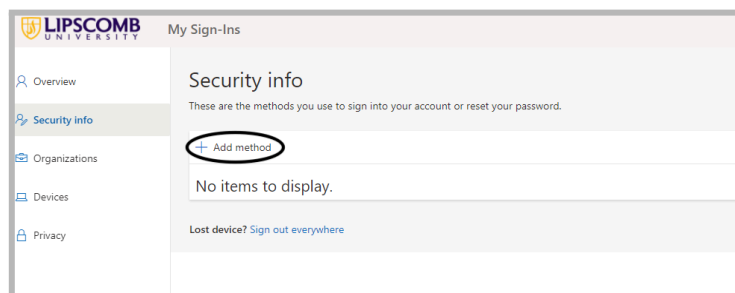
4. You should see this page. Under Security info, click “Update Info”



5. The page that appears will display any methods you have already set up for Password Reset or MFA. To remove a method that is no longer in use, click on the “Delete” link beside the method you wish to remove.



6. Click “+ Add Method” to add a new method.

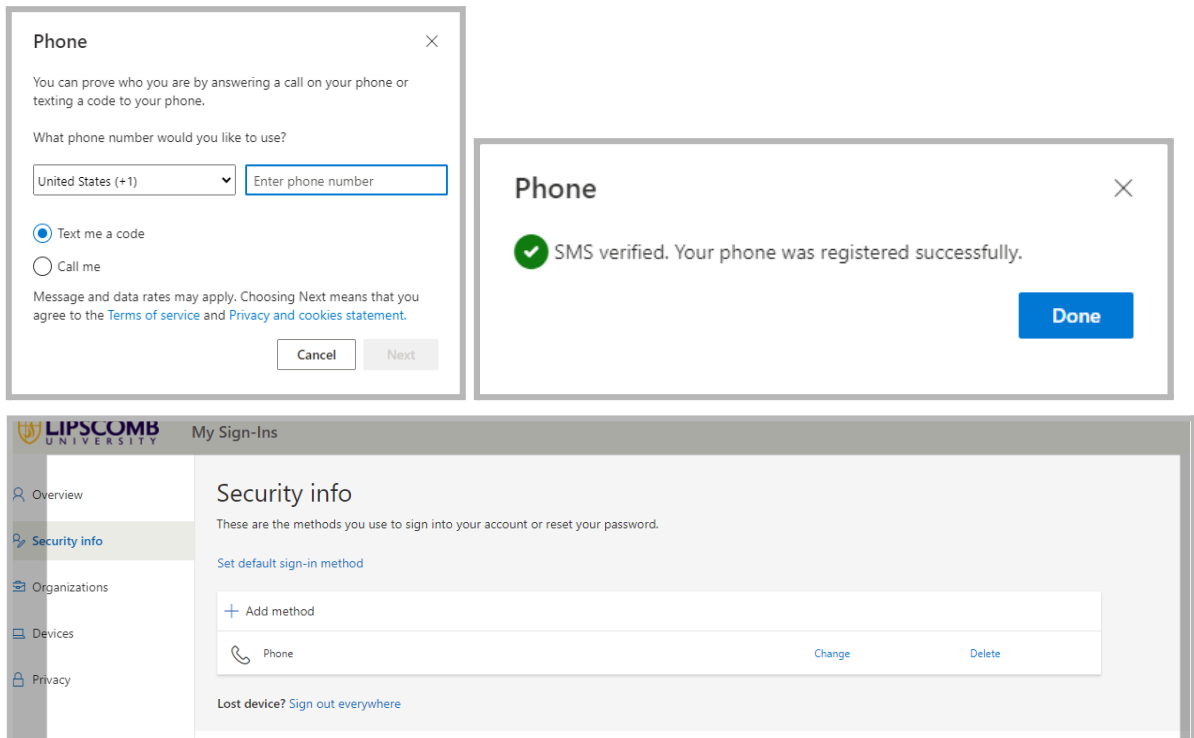


- a. We recommend setting up both your mobile phone (either text message or phone call) and an Authenticator App for this step so that you can have a backup method. Email and Security questions **will NOT work** for MFA as they are less secure—these options can only be set up for use with password reset.
- b. If you choose to use an authenticator app, you can use either the **Microsoft Authenticator App** or several others that are supported such as **Google, LastPass, and Duo Authenticator apps**.

Adding an Additional MFA Method

☐ Adding a Mobile Phone:

1. After you put in the number, it will text or call you with a code. After successfully entering the code, you will get a popup saying successful. After clicking Done it will take you back to the security methods page. Make sure the method you just set up is shown on the security page. (all pictured below)



The image displays two screenshots from the Lipscomb University 'My Sign-Ins' interface. The top-left screenshot shows a 'Phone' modal window where a user can select a country (currently 'United States (+1)') and enter a phone number. It offers two options: 'Text me a code' (selected) and 'Call me'. A 'Next' button is visible at the bottom right. The top-right screenshot shows a confirmation message: 'SMS verified. Your phone was registered successfully.' with a green checkmark icon and a 'Done' button. The bottom screenshot shows the 'Security info' page in the 'My Sign-Ins' dashboard. The page lists the added phone method with a 'Change' or 'Delete' link. A sidebar on the left contains links for Overview, Security info (active), Organizations, Devices, and Privacy.

☐ Adding an Authenticator App:

Download the App you wish to use to your mobile device - Microsoft Authenticator, Google Authenticator, Duo Mobile or LastPass Authenticator. This guide includes the setup instructions for the Microsoft and Google apps.

Microsoft Authenticator App Setup

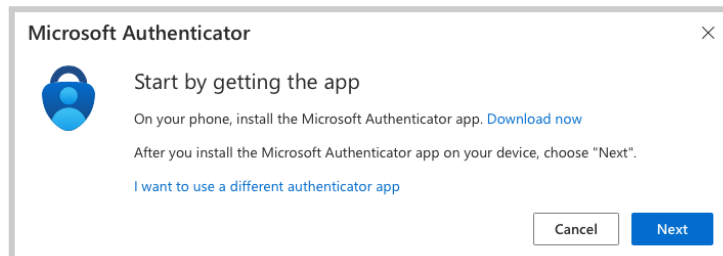


The process to setup the Microsoft Authenticator app can be done just using your mobile device **or** using a computer + mobile device. Each set of instructions are slightly different and detailed below:

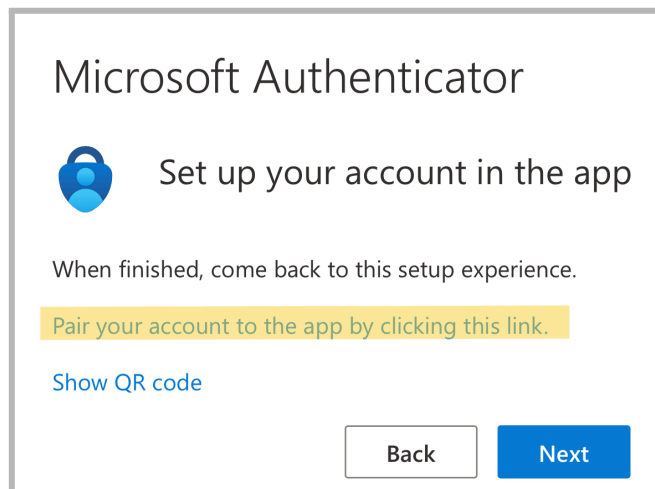
Note: The Authenticator app is tied to your physical mobile device. If you get a new phone, you'll need to set up a new authenticator app before you disable your old device, since the code will be sent to your old device first.

On a mobile device (only):

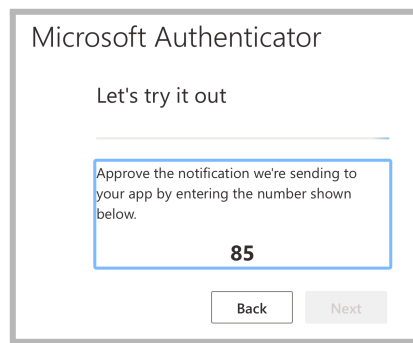
- ☐ Download the Microsoft Authenticator app from your phone's App Store before proceeding. (**Please Note: There are 'fake' authenticator apps. Be sure to check you are getting the official "Microsoft" one.*)
- ☐ Do Nothing with the newly downloaded app at this time.
- ☐ Open a browser on your mobile 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.



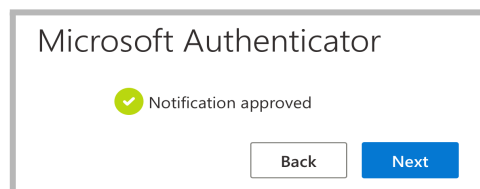
- ☐ You will see this screen. Click on the highlighted link that says "Pair Your account to the app by clicking this link"



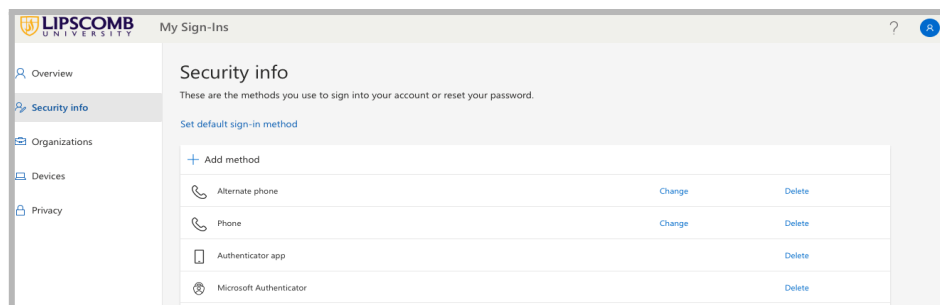
- ☐ Click on the highlighted link that says "Pair Your account to the app by clicking this link".
- ☐ It will automatically open the Authenticator app (*You may be asked to open the link in the app. Tap 'Open'.*)
- ☐ Go back in your web browser, tap 'Next'. You will now be asked to test your MFA setup. "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.

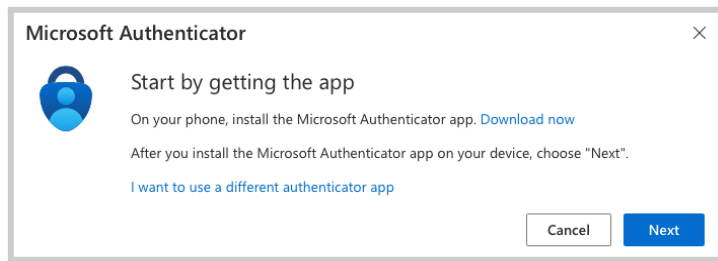


- ☐ You have now successfully configured Microsoft Authenticator to secure your account.
- ☐ You will see a brief popup that the app was successfully set up and 'Authenticator' or 'Microsoft Authenticator' will be displayed as a registered method when you return to the security page.

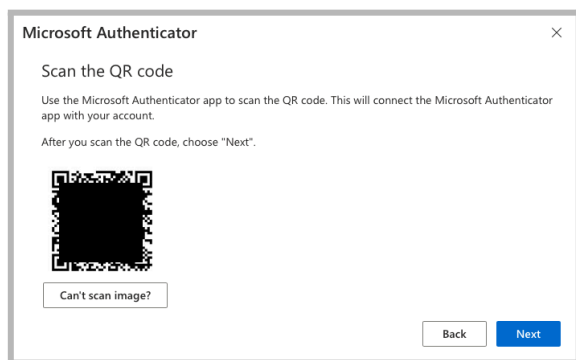


On a computer + mobile device:

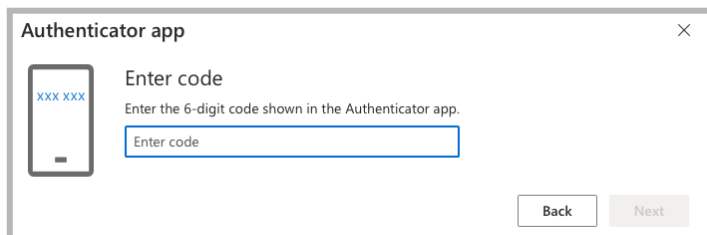
- ☐ Download the Microsoft Authenticator app from your phone's App Store before proceeding. (**Please Note: There are 'fake' authenticator apps. Be sure to check you are getting the "Microsoft" one that matches the logo above.*)
- ☐ Open a browser on your computer, such as Safari or Chrome. Go to the 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.



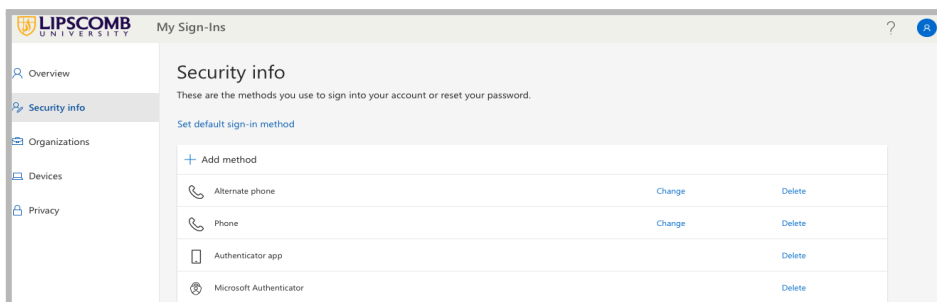
- ☐ Once you've downloaded the app on your smartphone, click on the 'Next' button as seen in the image above. You will be prompted to set up your account on the app on your mobile device.
- ☐ On your mobile device in the Authenticator App, click the + sign in the upper corner and choose Work or school 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.

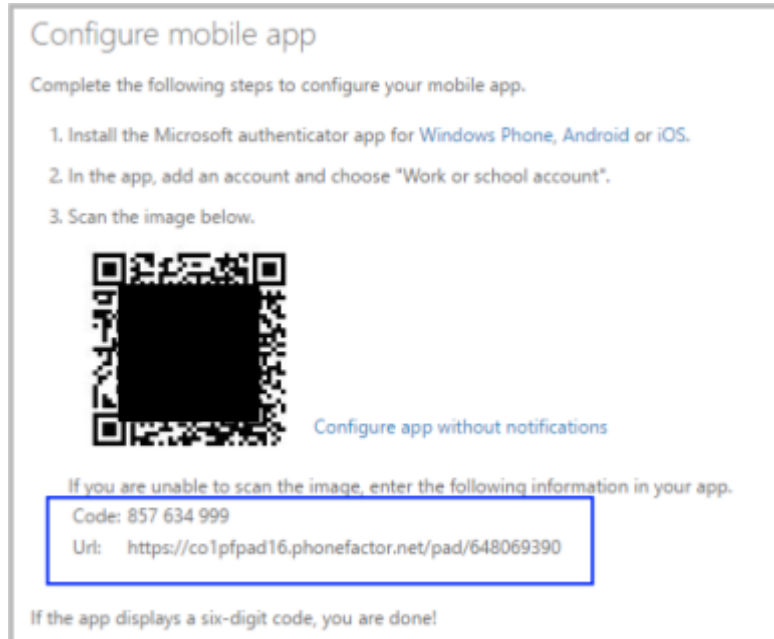


- ☐ Once you've scanned the QR code and clicked Next, it will test the connection with a prompt from the app – click 'Approve'.
- ☐ You will see a brief popup that the app was successfully set up and 'Authenticator' or 'Microsoft Authenticator' will be displayed as a registered method when you return to the security page.

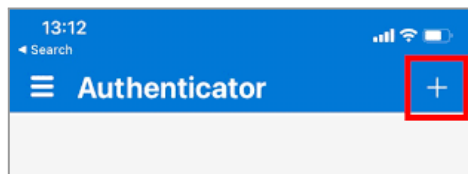


No QR Code to scan:

- ☐ 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**.



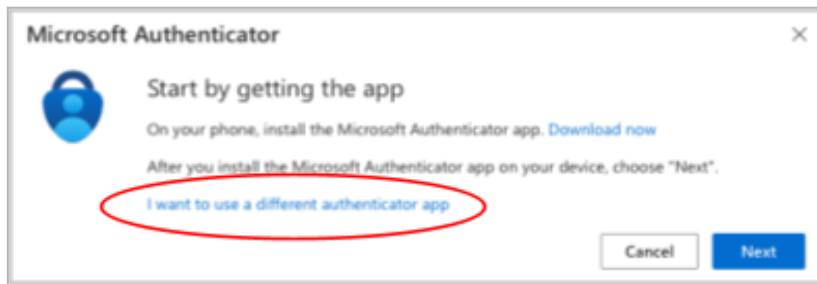
- ☐ Select **"ENTER CODE MANUALLY"**.



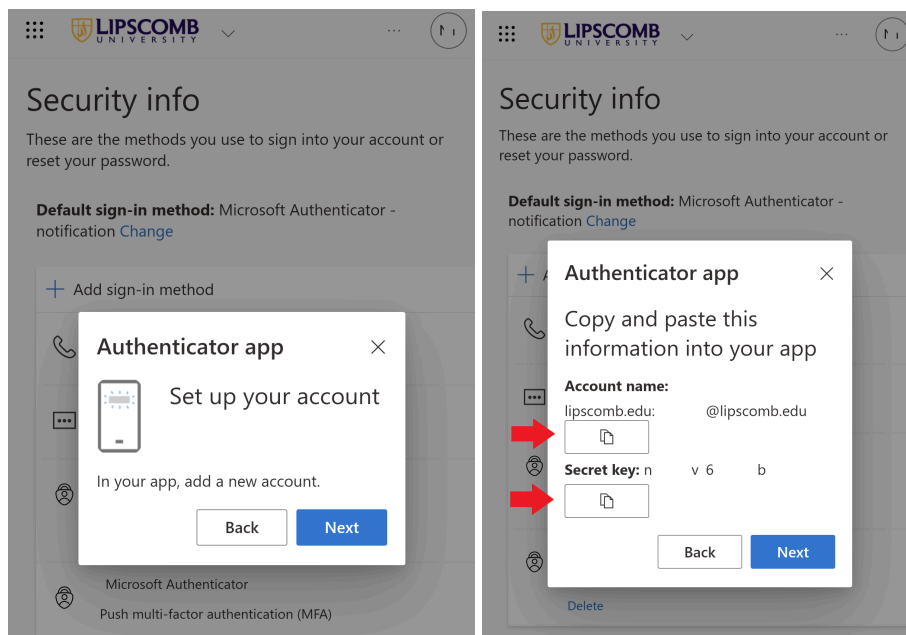
- ☐ Enter the Code and URL and then select **Finish**.

Google Authenticator App Setup

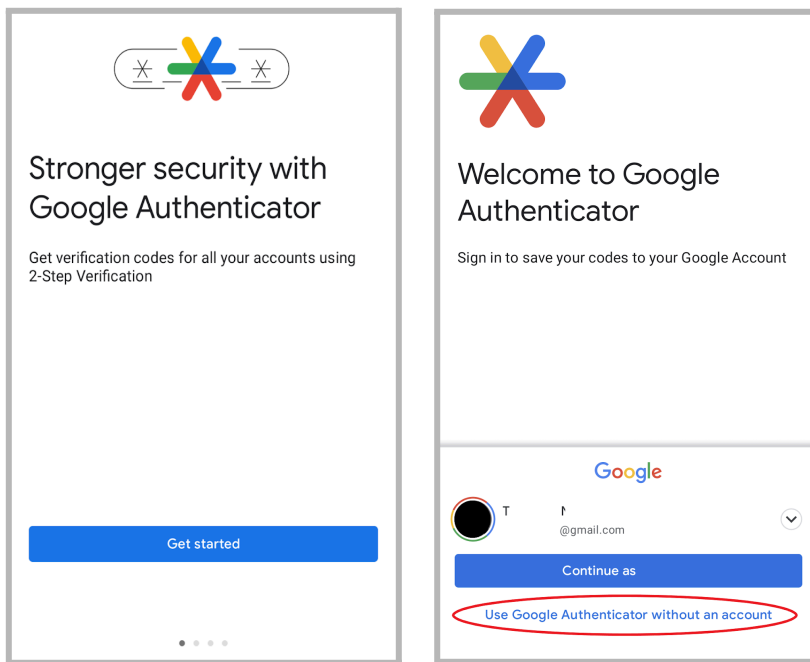
1. Download the Google Authenticator app from your phone's App Store before proceeding.
2. When setting up the app, you should be in the process of accessing the my.Lipscomb Portal for the first time (or after an IT reset), or already logged into your my.Lipscomb account.
3. When you are prompted during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



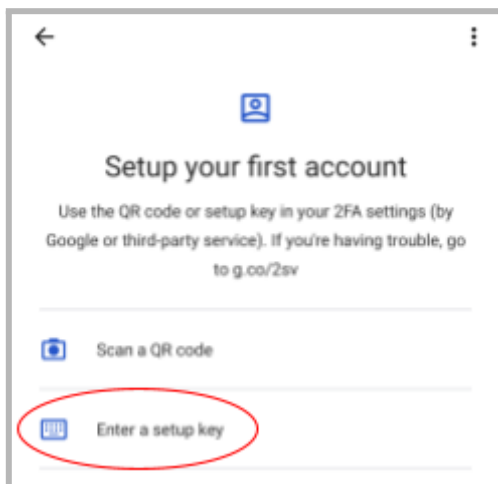
4. After you select "...use a different app", I will ask you to 'setup your account'. Click Next. On the following screen, you will have 2 items: your Account Name and your Secret Key. Keep this screen available, but you will need to change screens here.



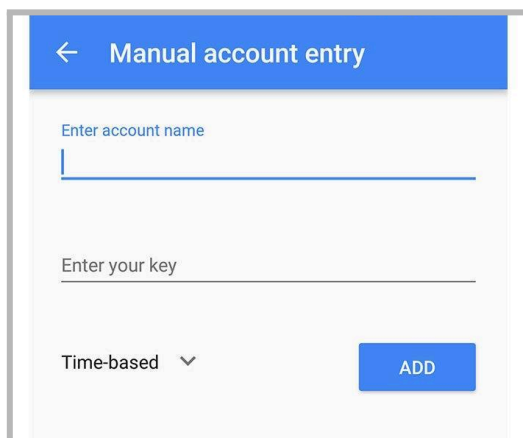
5. Go to your Google Authenticator app that you've downloaded on your smartphone.
6. Click on the "Get Started" button as seen in the image below. You will be prompted to sign in with a Google Account. Instead, **click on "Use Google Authenticator without an account".**



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



8. 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.



If you can't log in:

If you are on campus, you can come by the IT Help Desk in the lower level of Beaman Library with a photo ID to confirm your identity.

If you are remote, you can send a photo of yourself holding your ID (either your Lipscomb ID or a state-issued ID) beside your face to helpdesk@lipscomb.edu along with your mobile phone number. Your name on the ID must be high enough resolution that it is readable.

Once your identity is verified, we will assist with setting up your new MFA settings using the contact information in your student or employee record.

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.