New Students: Set Up Your SEU Account

Welcome to Southeastern University! This guide will help you set up your Single Sign-On (SSO)/Multi Factor Authentication (MFA) for your SEU account.

Table of Contents

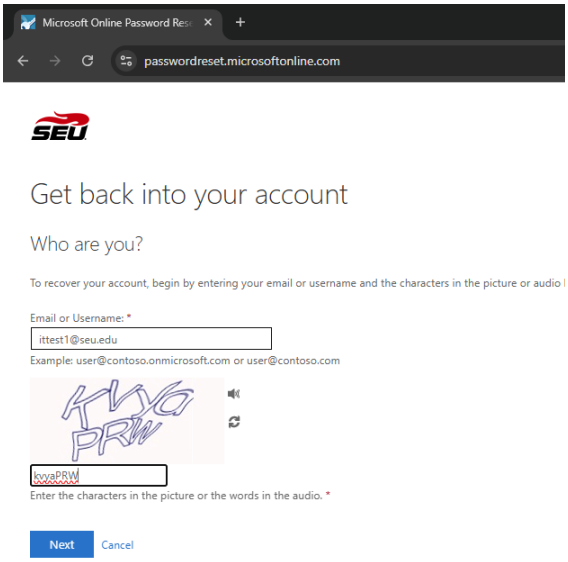
1: Create a password

To begin with your SEU account, you need to make a password. As of 9/10/2025, here are our password requirements:

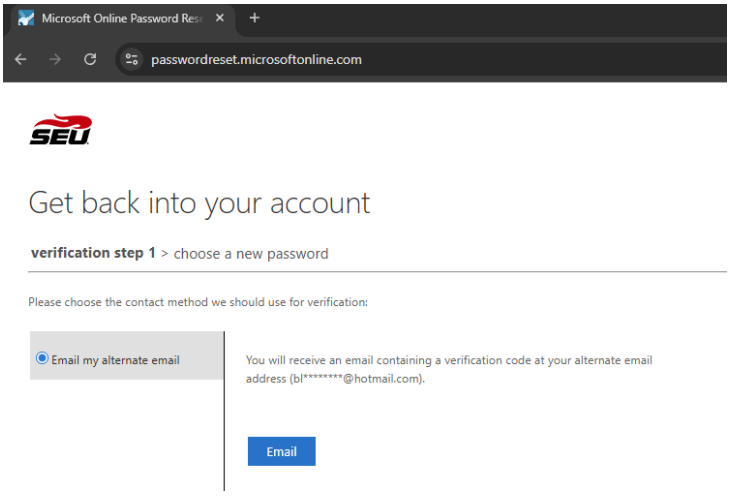
1. It must be at least 20 characters. Phrases are acceptable.
2. Do not include words relating to the school, i.e. SEU, southeastern, etc. You may receive an error.
3. Avoid common phrases and psalms. You may receive an error if Microsoft recognizes if parts of it are too commonly used.
4. Come up with something unique to you that you will remember. Save it in a secure personal password manager, if needed.
5. Do not share your password. No one, not even IT, should be asking you for your SEU password.
6. Going forward, you cannot reuse your last 10 passwords.

How to create your first SEU password:

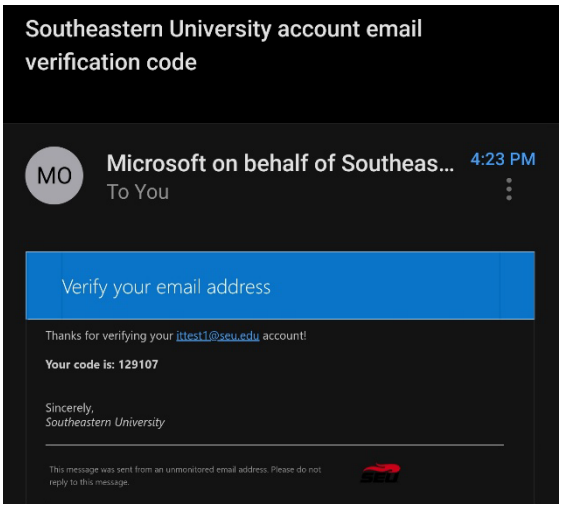
1. Go to the self-service password recovery link: Password setup
2. Enter your **SEU email address** that you received in your welcome email. Then, fill out the CAPTCHA prompt and select **Next**.



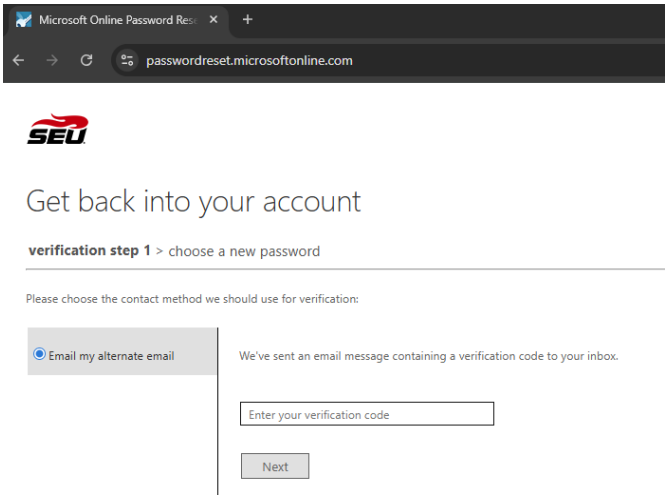
3. You will be prompted to send an email containing a verification code to your **PERSONAL EMAIL**. This will be the email you used when you applied to SEU. Select **Email**.



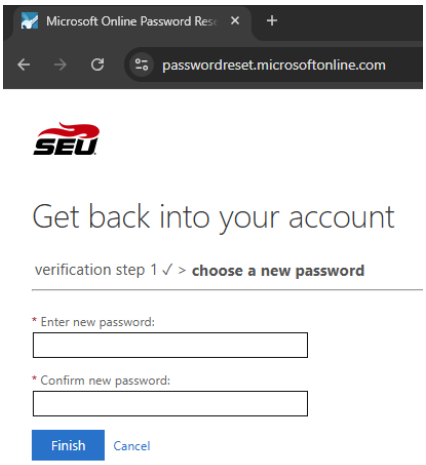
4. Check your personal email for an email from msonlineserviceteam@microsoftonline.com that contains a code. You will need it for the next step.
    a. NEVER share this code with anyone, especially anyone over the phone. In the future, if someone asks you for this code, please reset your password and/or reach out to the SEU IT Help Desk.



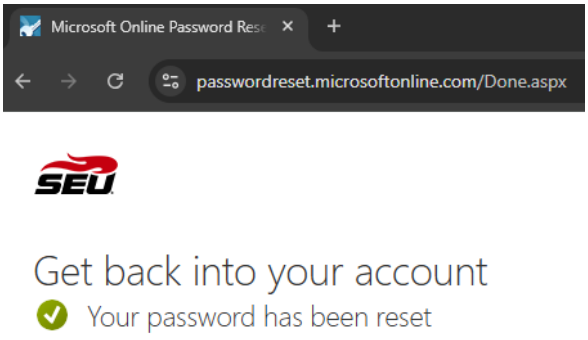
5. Enter the **code** you received in the email and select **Next**.



6. Create a password based on the password policy listed above and select **Finish**.



7. When prompted that your password has been reset, you may close this browser tab. The next sections will walk you through setting up MFA on your account and accessing your SEU My Apps dashboard at https://myapps.microsoft.com.



2: Choose your MFA option

To access your SEU Microsoft account, you must have **at least one** of the following MFA methods set up:

1. Microsoft Authenticator
2. Phone (SMS)
3. Another authenticator app

Please see each section's pros and cons to determine which MFA method(s) are right for you.

2.1: (Option 1) Microsoft Authenticator App

The Microsoft Authenticator app is SEU IT's recommended MFA method. It sends a notification to the Microsoft Authenticator app to your phone when you log into your SEU account. Type in the two-digit number into your app and you gain access to your account.

Pros:

1. The push notification allows for the fastest and most secure login option.
2. You have the option to view an offline, 6-digit code if your phone has no internet or data connection.

Con:

1. If you replace your phone, you will either need to use a backup MFA method to access your account, such as Phone (SMS), or contact the SEU IT Help Desk during business hours.

You can set up the Microsoft Authenticator app from just your phone, or by using your phone and your computer. Both paths have the same result: You will set up the Microsoft Authenticator app on your mobile device and use that lo log into your SEU account going forward.

2.1.1: (Option 1) Set up your account *from* a **phone**

These steps will assist you in setting up your MFA all from your phone – no QR code scanning or second device required to display a QR code.

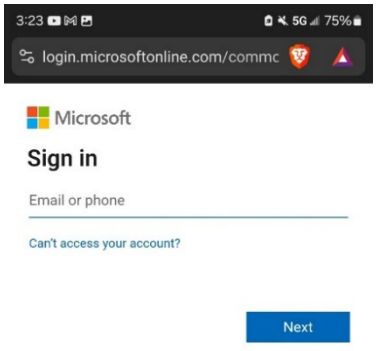
If you are having issues with setting up your MFA using just your mobile device, you can log into your Microsoft account on a computer instead – instructions for that are in the next section.

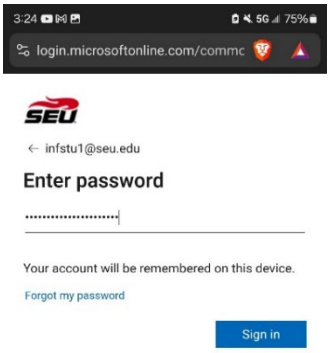
1. On your mobile device, go to the App Store (iPhone) or Play Store (Android) and search for **Microsoft Authenticator**. Verify that the app developer is Microsoft Corporation and install the app.

2. Open the **Microsoft Authenticator** app. If prompted at any point in the setup process, **allow** for push notifications.

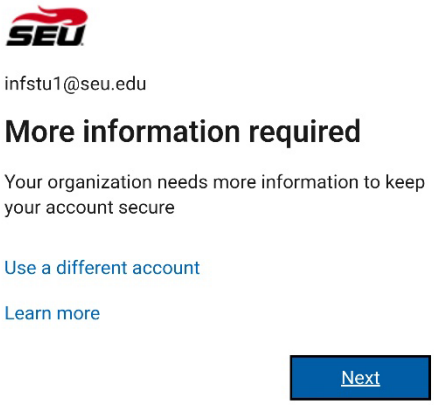
3. Open a mobile web browser, such as Safari or Chrome and go to https://myapps.microsoft.com.

4. Enter your SEU email address and SEU password to sign in.

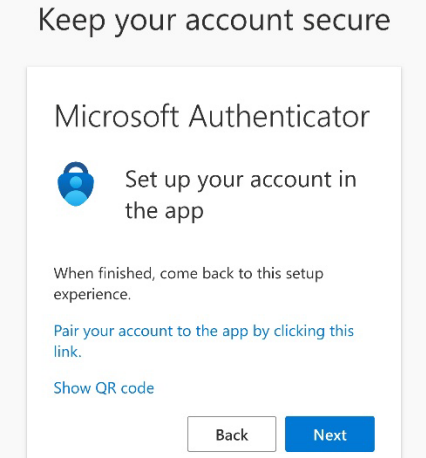




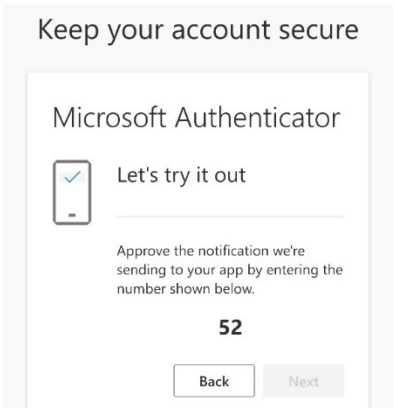
5. When prompted for **More information required**, select **Next**. At the **Start by getting the app** screen, select **Next**.

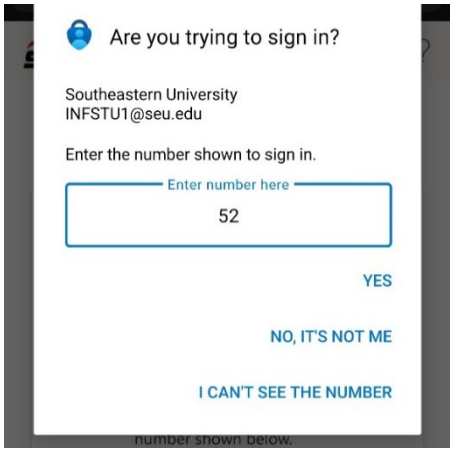


6. At the **Set up your account in the app** screen, select **Pair your account to the app by clicking this link**. Microsoft Authenticator will pop up and may ask you to unlock the screen. When it prompts you that the **Account added successfully**, you will see your SEU account listed in the Microsoft Authenticator app. **Switch back to your mobile browser app** and select **Next**.

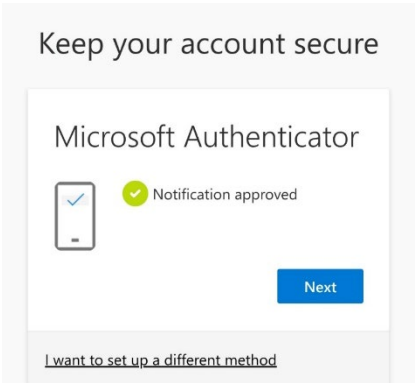


7. Take note of the number on-screen. You will receive a push notification from the **Microsoft Authenticator** app. Click on it or switch back to the app to enter the number. Select **Yes**.





8. Once the notification is approved, select **Next**.



9. You should be directed to your SEU My Apps dashboard. If not, then go to https://myapps.microsoft.com and log in if prompted. For more information on your dashboard, see section **5: Accessing your application dashboard and important links.**

10. You have successfully set up Microsoft Authenticator. If you replace your phone, you will either need to use a backup MFA method to access your account, such as Phone (SMS), or contact the SEU IT Help Desk during business hours. To set up Phone (SMS) as another login method, please see the steps later in this document on how to add it.
    a. **IMPORTANT**: Please DO NOT delete/uninstall the Microsoft Authenticator app from your mobile device. You will need it for each time you need to log into your SEU account.

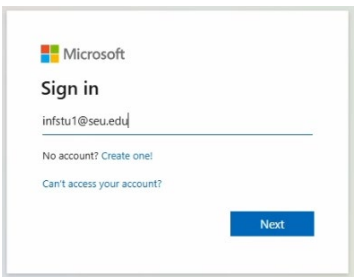
2.1.2: (Option 1) Set up your account *from* a **computer**

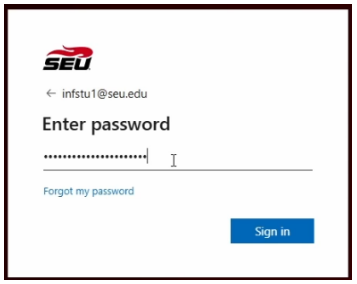
Please note that you will still need your mobile device to download the app and use it.

If you are having issues with setting up your MFA from just your mobile device, you can log into your Microsoft account on a computer instead.

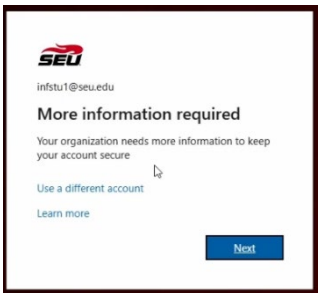
1. On your computer, go to https://myapps.microsoft.com.

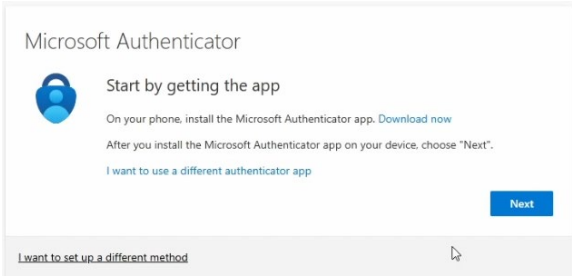
2. Enter your SEU email address and SEU password to sign in.





3. When prompted for **More information required**, select **Next**. At the **Start by getting the app** screen, select **Next**.

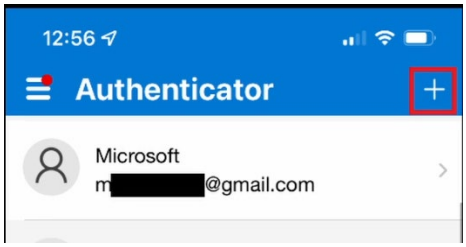


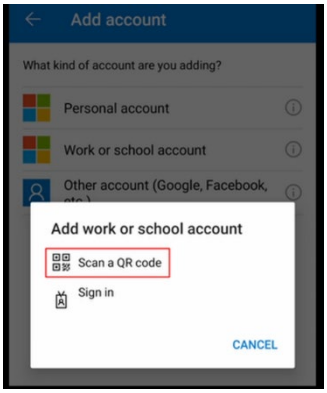


4. On your mobile device, go to the App Store (iPhone) or Play Store (Android) and search for **Microsoft Authenticator**. Verify that the app developer is Microsoft Corporation and install the app.

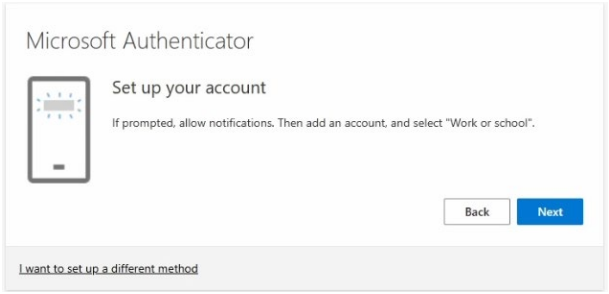
5. On your mobile device, open the **Microsoft Authenticator** app. If prompted at any point in the setup process, **allow** for push notifications.

6. In **the Microsoft Authenticator** app, select the **+** icon, then select **Scan a QR code**. If prompted, allow the app to have camera access.

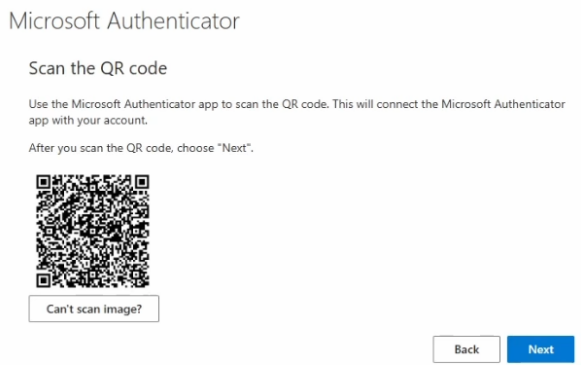




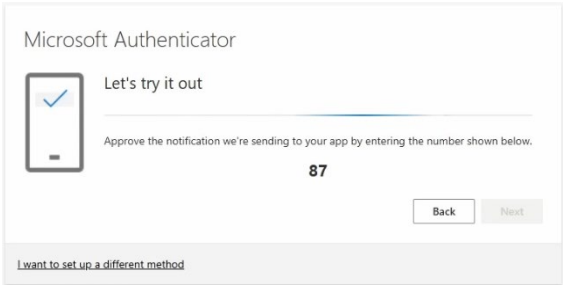
7. On your computer, at the **Set up your account in the app** screen, select **Next**.

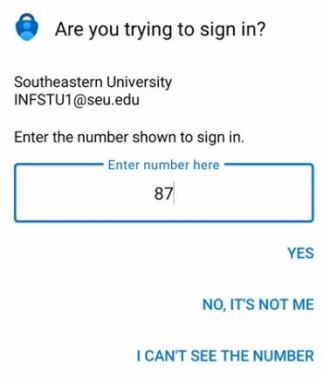


8. Use your phone camera to scan the QR code. When you see that the **Account added successfully** on your phone, select **Next** on your computer.

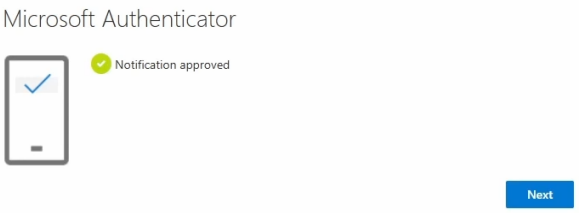


9. Your mobile device will receive a push notification from the **Microsoft Authenticator** app. Click on the notification or open the app to type in the code you see on-screen. Select **Yes** on the app.





10. When you see that the notification is approved, select **Next**.



11. Select **Done**. You should be directed to your SEU My Apps dashboard. If not, then go to https://myapps.microsoft.com and log in if prompted. For more information on your dashboard, see section **5: Accessing your application dashboard and important links.**
12. You have successfully set up Microsoft Authenticator. If you replace your phone, you will either need to use a backup MFA method to access your account, such as Phone (SMS), or contact the SEU IT Help Desk during business hours. To set up Phone (SMS) as another login method, please see the steps later in this document on how to add it.
    a. **IMPORTANT**: Please DO NOT delete/uninstall the Microsoft Authenticator app from your mobile device. You will need it for each time you need to log into your SEU account.

2.2: (Option 2) Setup with Phone (SMS), aka text messaging

This Phone (SMS) MFA method will allow you to receive a text message with a code when you sign into the SEU account. This is useful as most people are less likely to replace their phone number, whereas replacing your phone is more common. However, there are still drawbacks.

Pro:

1. If you don't change your phone number, the Phone (SMS) option acts as a long-term MFA method.

Cons:

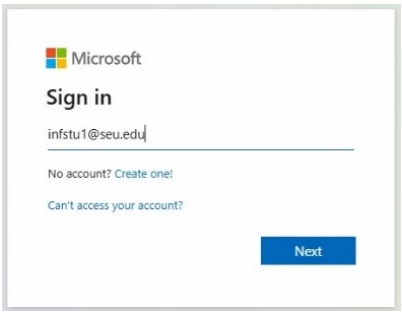
1. **Text messaging is entirely reliant on your own cellular service**. If you are in a location that does not get good cell reception, then you are less likely to get the text with the code you need to log into your account. Using the Microsoft Authenticator app or even another authenticator app makes it so that even if your phone has no cellular, data, or internet connection, you can still log into your SEU account.
2. This is not the fastest way to log in. The notification from Microsoft Authenticator makes logging in much quicker and more secure.

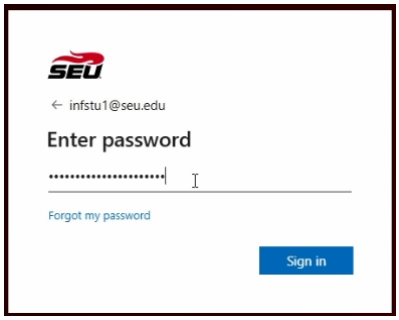
Set up Microsoft MFA with Phone (SMS):

The following instructions assume you are performing the setup from a computer. However, you can set up Phone (SMS) for MFA from a mobile device. You will just need to switch back and forth between your phone's mobile web browser and text messaging (SMS) app when you get to the relevant steps. If you are having difficulties with the differences, then simply follow the instructions below.

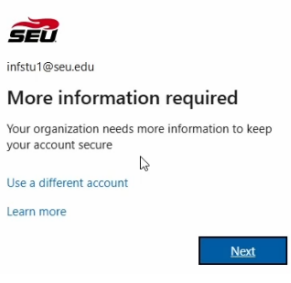
1. On your computer, go to https://myapps.microsoft.com.

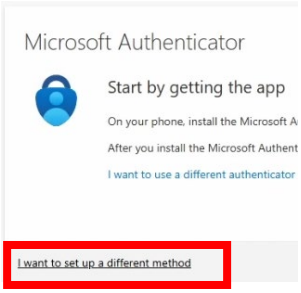
2. Enter your SEU email address and SEU password to sign in.

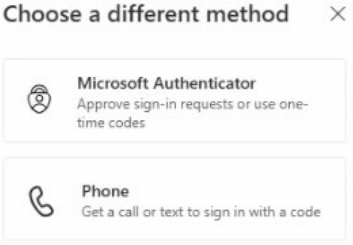




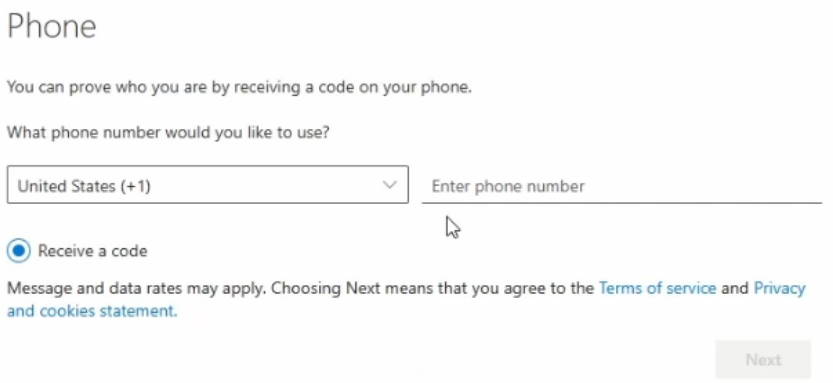
3. When prompted for **More information required**, select **Next**. Select **I want to set up a different method**, then select **Phone**.





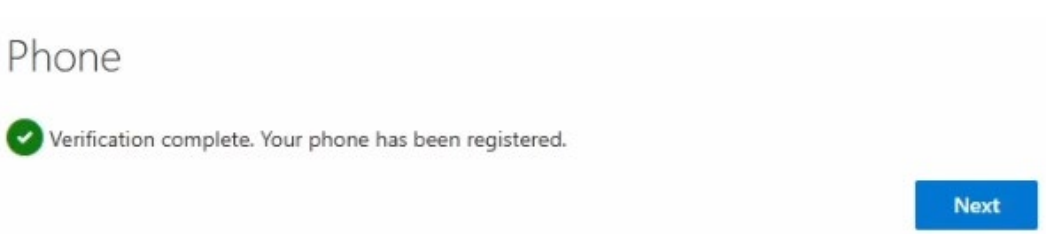


4. Choose your country code, then enter your full cell phone number and select **Next**.



5. Your cell phone will receive a text with a 6-digit code. Enter it here and select **Next**.

6. You are finished setting up Phone (SMS) as your MFA method. If you change your phone number, you should contact the SEU IT Help Desk.



7. Select **Next** and **Done**. You should be directed to your SEU My Apps dashboard. If not, then go to https://myapps.microsoft.com and log in if prompted. For more information on your dashboard, see section **5: Accessing your application dashboard and important links.**

2.3: (Option 3) Setup with a third-party MFA app

To use a another MFA app such as Google Authenticator or FreeOTP, you would choose ***I want to use a different authenticator app*** during MFA setup.

Pros:

1. Some apps, like FreeOTP, are more lightweight and make it easier to manage MFA tokens.
2. Some apps, like Google Authenticator, allow you to log into a personal account and sync your MFA tokens over to new devices. You must keep good track of this if you choose to do this as it is not always reliable.
3. Any MFA app is a more secure login method than Phone (SMS).
4. You have the option to view an offline, 6-digit code if your phone has no internet or data connection.

Cons:

1. Push notifications are not supported, resulting in slower logins. For push notifications, use Microsoft Authenticator.
2. Some apps are better than others; the choice is yours.
3. If you replace your phone, you will either need to use a backup MFA method to access your account, such as Phone (SMS), or contact the SEU IT Help Desk during business hours.

While this option is available to you, it is not documented because each authenticator app differs from one another, even though they generally perform the same function in providing a 6-digit OTP code. They will funtion similarly to the Microsoft Authenticator app, except with no push notification.

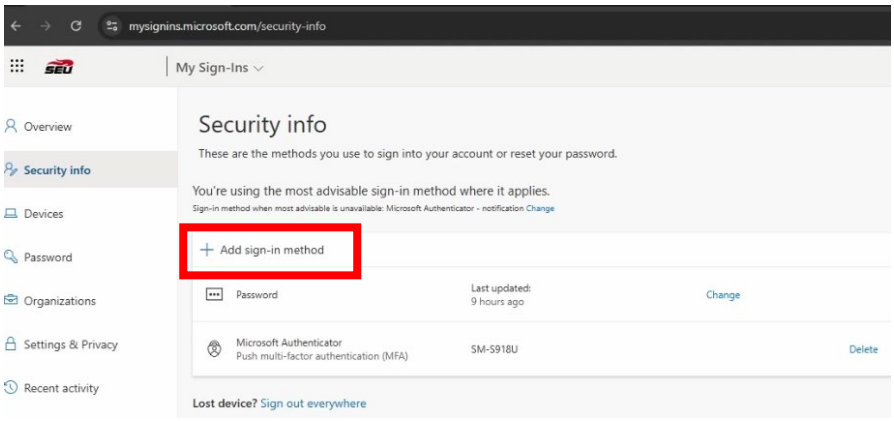
4: Set up personal email for password recovery

Your new account should have a personal email for password recovery. However, if it does not have one, or you would like to add a new one, you may do so. You will not be able to use a personal email as an MFA method or to reset your MFA method. If you need to reset your MFA method because you no longer have access to it (changed phone or phone number) then please reach out to the SEU IT Help Desk at (863) 667-5028 during business hours.

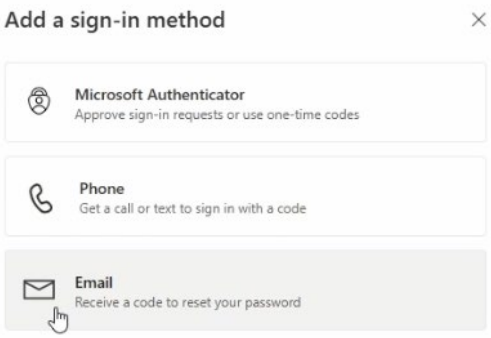
To set up a personal email for password recovery:

1. Please go to your Microsoft account's Security info screen and log in if prompted: https://mysignins.microsoft.com/security-info

2. Select Add sign-in method.

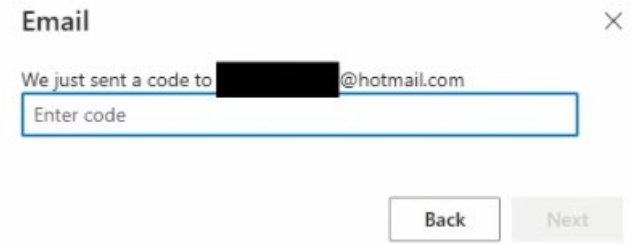


3. Choose Email.

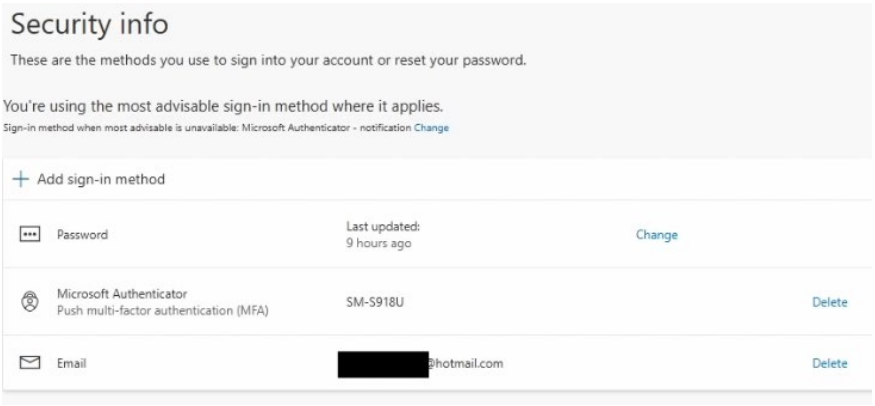


4. Enter a personal email address. This cannot be an SEU email address. Select **Next**.

5. You will receive an email from Microsoft with a 6-digit code in your personal email inbox. It may take a minute to receive it. When you do, enter it here and select **Next**.

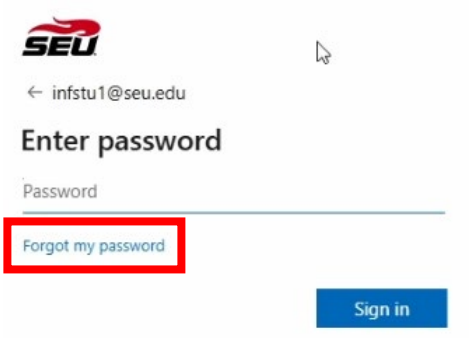


6. You now have a personal email set up for self-service password recovery.



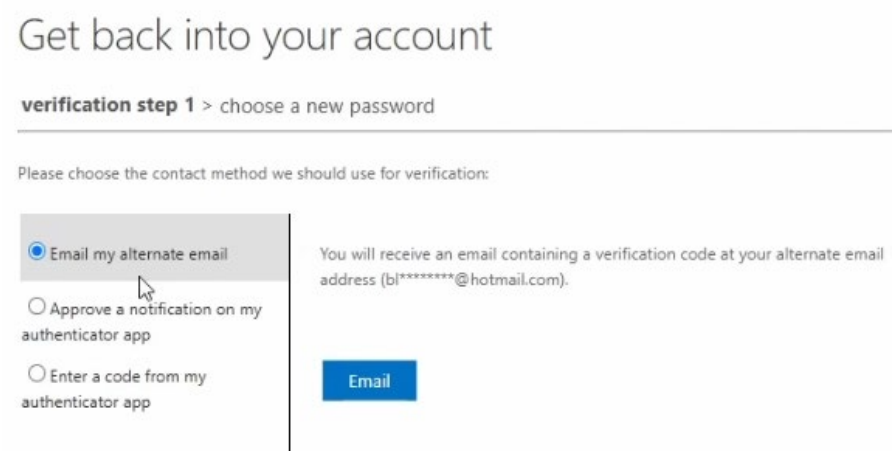
4.1: How to reset a forgotten password

1. At the screen where you need to enter your SEU password, select Forgot my password.

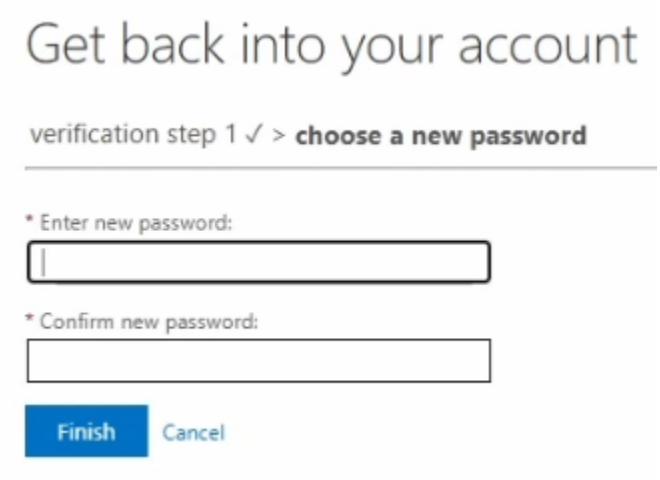


2. Enter your SEU email address, solve the CAPTCHA prompt, and select **Next**.

3. Select any of the available recovery methods for your account.



4. Once you have verified with whatever method you chose, you can change your SEU password. As of September 2025, it still must be at least 20-characters long and cannot match any of your previous 10 passwords. Select **Finish**.

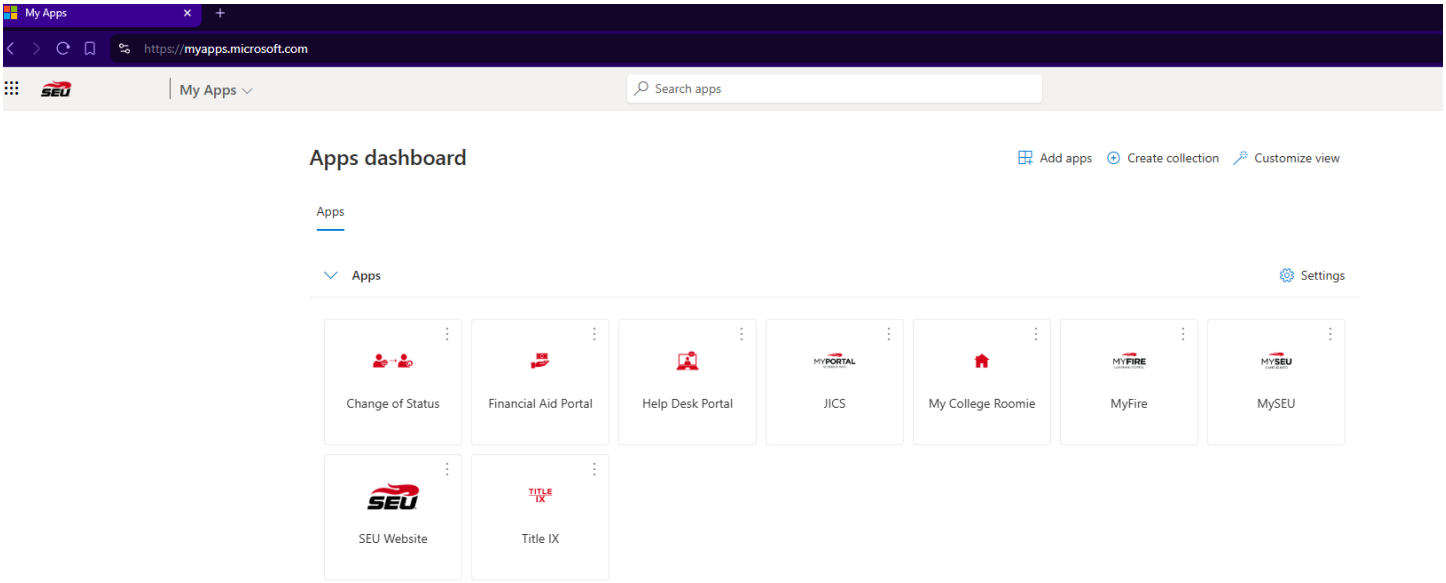


5. If you have any issues resetting your password, please reach out to the SEU IT Help desk at (863) 667-5028.

5: Accessing your application dashboard and important links

5.1: SEU My Apps dashboard (Microsoft Entra Application Portal)

SEU My Apps dashboard : https://myapps.microsoft.com



From your dashboard, you can access your SEU applications. This includes, but is not limited to, your SEU email, MyFire, and JICS.

For most apps, like JICS, you can click on its tile and it will log you in.

5.2: Manage your account's MFA methods

Another important page for you is your Microsoft account's Security info.

Microsoft Security info: https://mysignins.microsoft.com/security-info

From here, you can manage your MFA methods and your personal email for password recovery. Check here periodically. If you have old phones, phone numbers, or emails in there, you should remove them.