Purpose

Multi-factor authentication (MFA) involves something you know (your username and password) and something you have (your phone). After you set up your multi-factor authentication, you will continue to use the same username and password, but you will also be prompted to provide an additional verification that you are currently trying to sign in. This extra layer of security prevents anyone but you from logging in to your account, even if they know your password. A common example would be a verification code sent via text to your cell phone when you try to log on, which you then have to enter before access is granted.

Information/Instructions

Is MFA Required?

To protect student and employee data, MFA is mandatory for all faculty, staff, and work-study employees as of Tuesday, March 31st, 2020, to access all OTC systems when outside of the College's computer network. These services include, but are not limited to, myOTC, email, Canvas, Zoom, and Microsoft Teams.

If multi-factor authentication has been turned on for you and you have not yet set up your preferred method of authentication, you may get an error message when trying to sign into an OTC system that utilizes single sign-on (SSO).

Device Overview

	Smartphone	Cell Phone	Landline	Tablet	Hardware Token
Push notifications via Microsoft Authenticator App	X			X	
Text Message (SMS)	X	X			
Phone Call	X	X	X		
Verification code	X			X	X

- **Smartphone:** Using a smartphone with the Microsoft Authenticator app lets you use MFA in four different ways. You can receive:
    1. Push Notification – An automatic notification is sent to your phone
    2. Text Message (SMS) – A passcode is sent vis SMS text.
    3. Phone calls – Your phone is automatically called.

4. Verification codes – The app can generate a verification code.

   No cell reception or WiFi? Once installed the Microsoft Authenticator app can generate a verification code without requiring a cell signal or the internet.

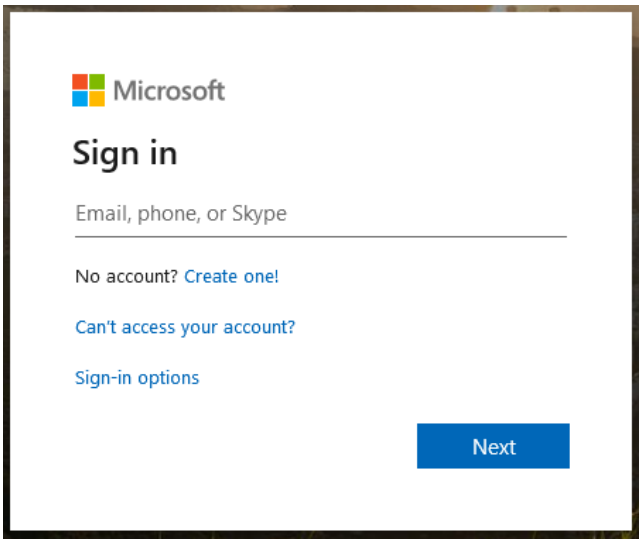
- **Cell Phone:** Can be called as a phone or used to receive SMS text message.
- **Landline:** A telephone call to any landline phone will prompt for approval or denial of the log on attempt.
- **Tablet:** Enroll your table to receive either push notification or verification codes via the Microsoft Authenticator app.
- **Hardware Token**: A small lightweight keyfob that can be attached to your key chain. Pressing the button on the keyfob will generate a verification for you to use with MFA. Tokens can be obtained by contact the Help Desk.

Instructions:

Set up your smartphone or tablet with the Microsoft Authenticator App:

You will need a computer, your smartphone or tablet, and your OTC username and password.

1. Install the Microsoft Authenticator app onto your smartphone
   - Android or iOS
   - Or search for **Microsoft Authenticator** in your smartphone's application store and install it.
2. Go to: http://aka.ms/mfasetup
3. When prompted, enter your OTC email address.



4. This will redirect you to an OTC sign-in page. **Sign in** with your OTC user name and password.

OZARKS TECHNICAL COMMUNITY COLLEGE

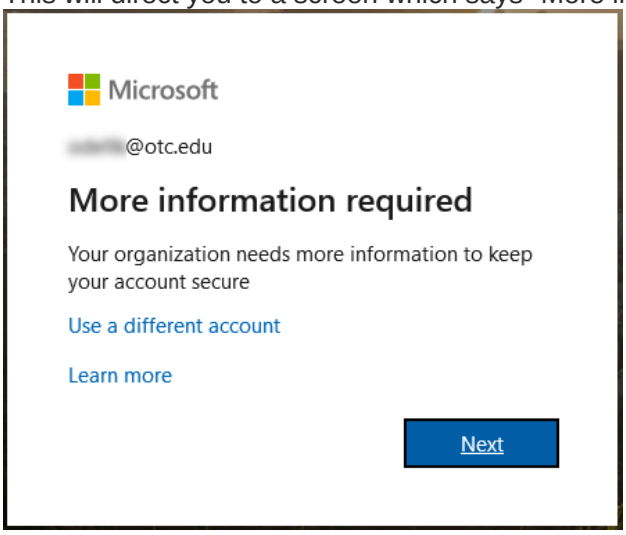
Please sign in with your OTC user name and password

[redacted]@otc.edu

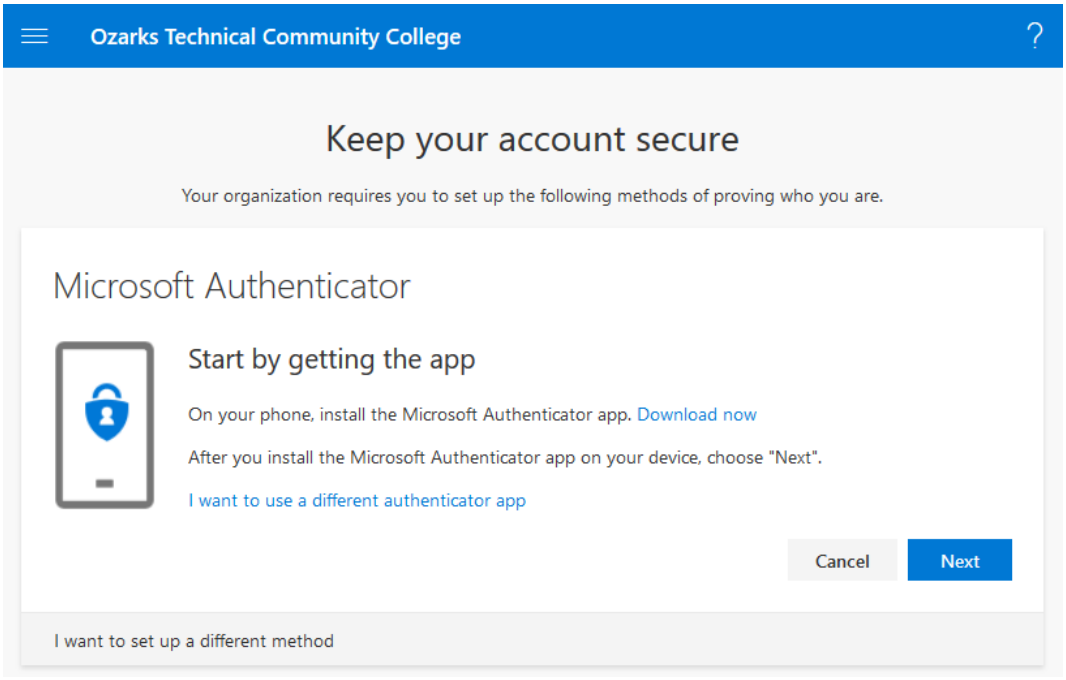
••••••••••••

Sign in

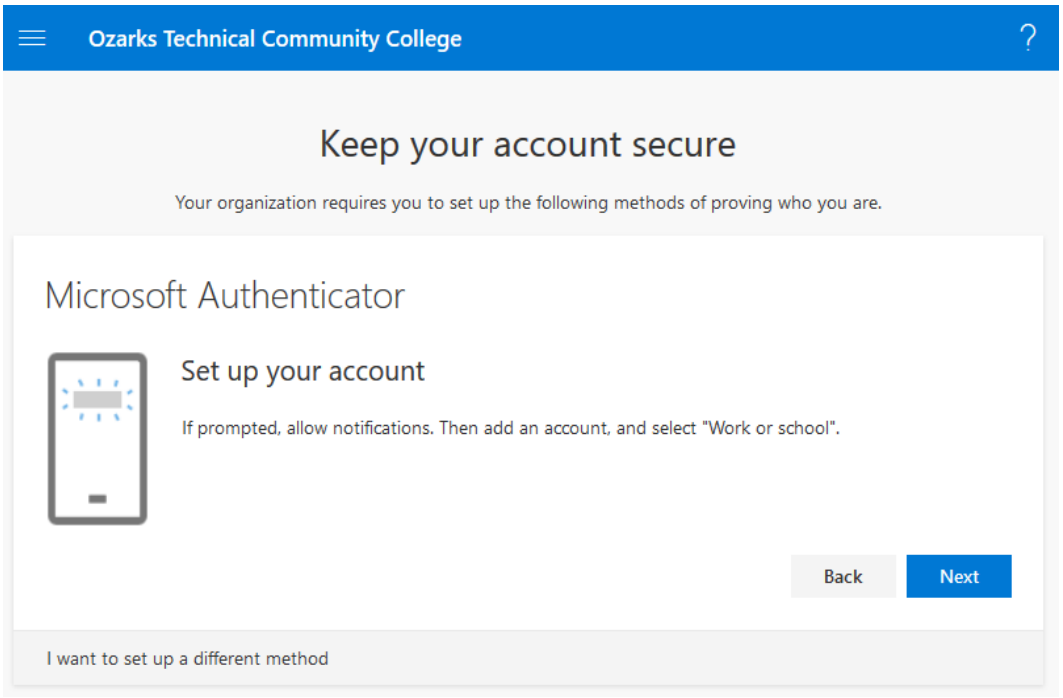
5. This will direct you to a screen which says "More information required." Click **Next**.



6. By default, the Microsoft Authenticator app is suggested. Since this should already be installed on your device, click **Next** to continue. (If it is not installed, install the app as directed above, and then click Next.)



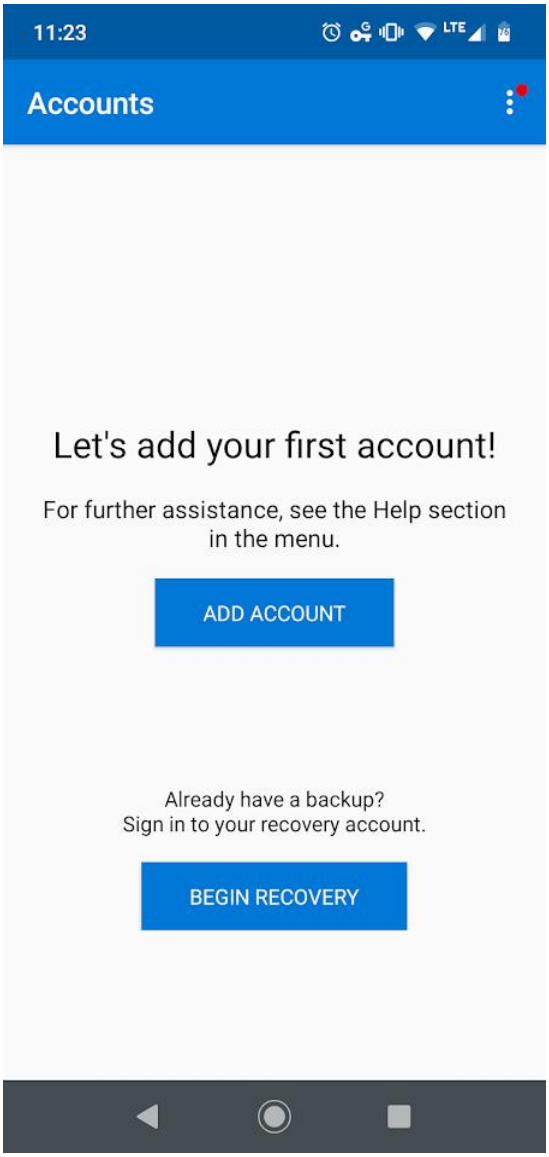
7. This will bring you to this screen (below), which directs you to set up your account in your new phone app.



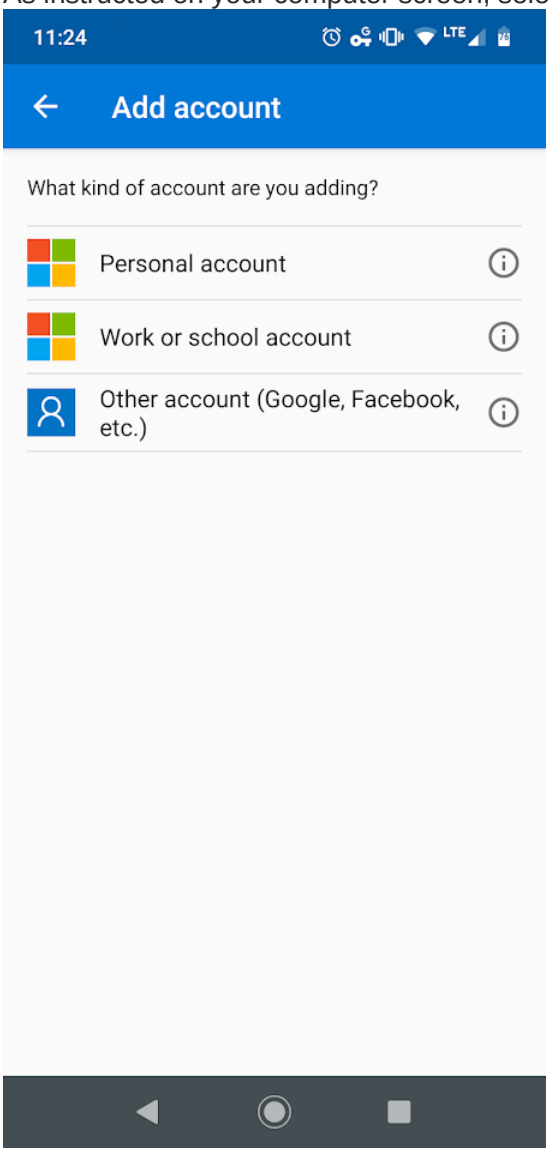
8. On your smartphone or tablet, open the Microsoft Authenticator app. Click through the prompts until you are able to click **Get Started**.

9. Click **OK** on the Data Privacy prompt, and we recommend clicking OK or Allow on any other prompts.

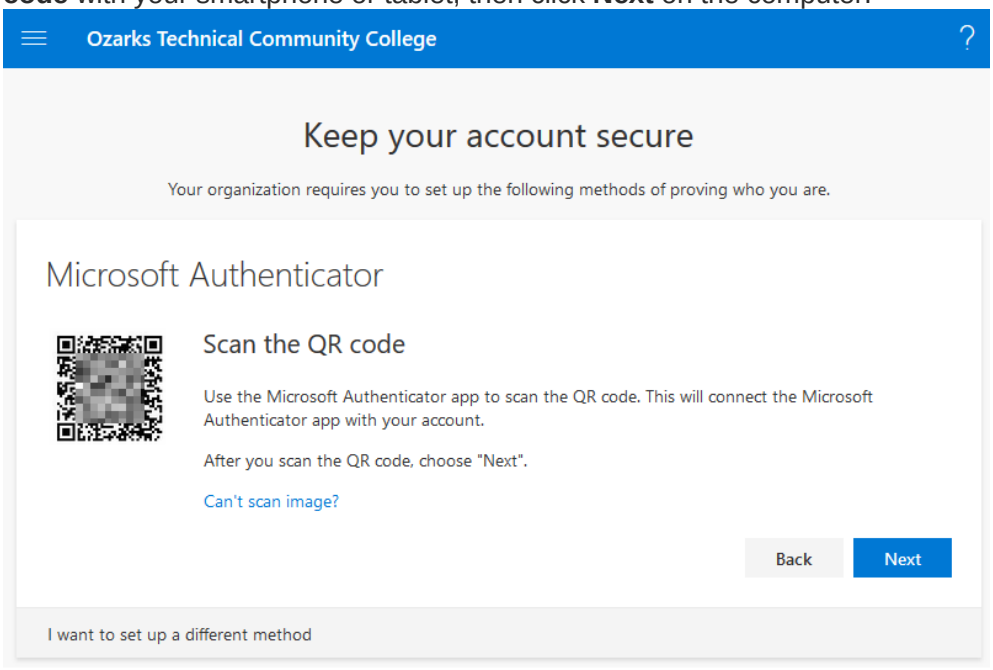
10. Select **Add Account**.



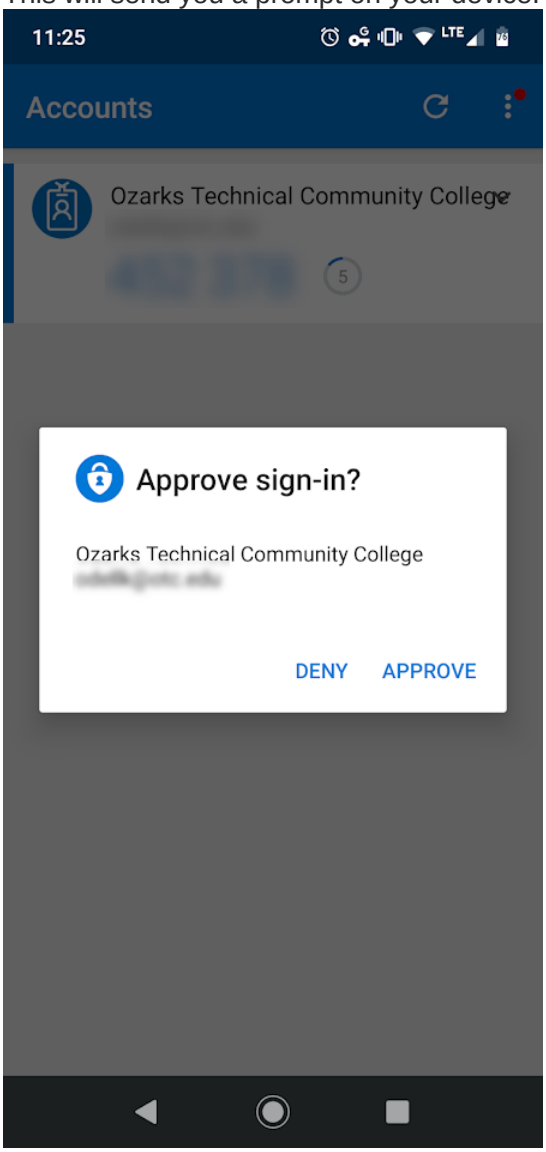
11. As instructed on your computer screen, select **Work or school account**.



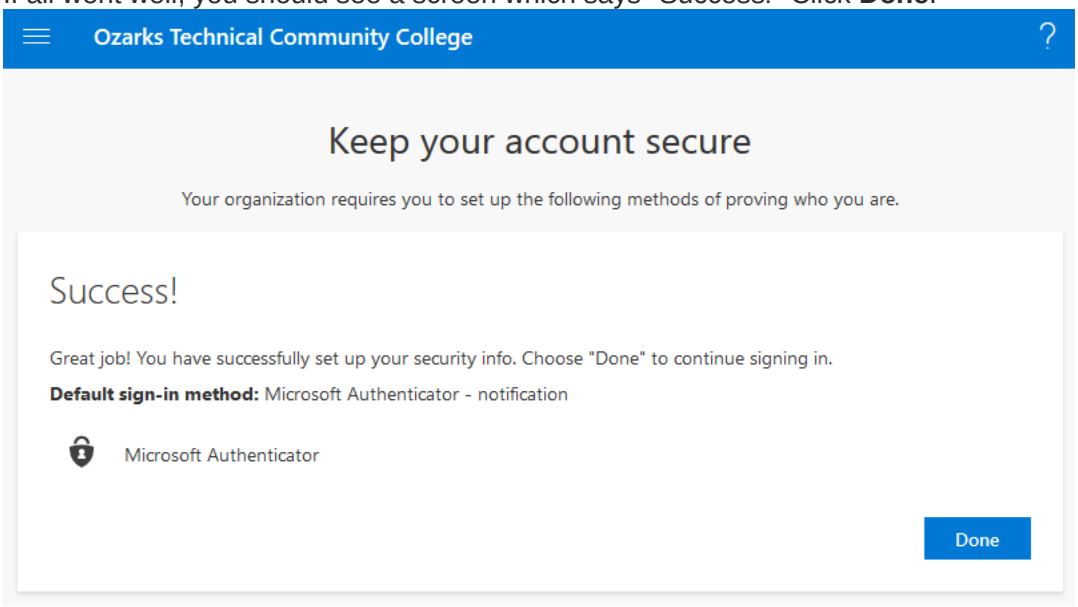
12. Click **Next** on your computer screen. This should display a QR code. **Scan the QR code** with your smartphone or tablet, then click **Next** on the computer.



13. This will send you a prompt on your device. Click **Approve**.



14. If all went well, you should see a screen which says "Success!" Click **Done**.



It is highly recommended that you have multiple devices configured for MFA. The more devices you use, the less likely you are to get locked out.

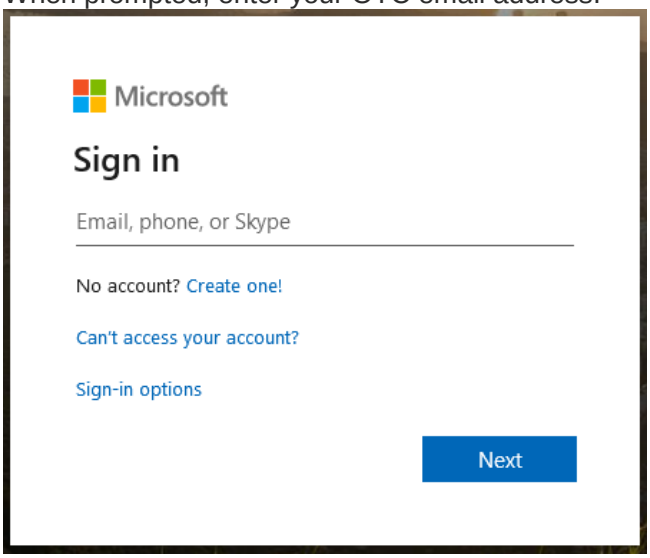
Set up your smartphone or basic cell phone with SMS verification:

This method supports receiving SMS text messages for MFA verification or a phone call as a backup method. These directions assume a cellular network connection to receive the SMS texts.

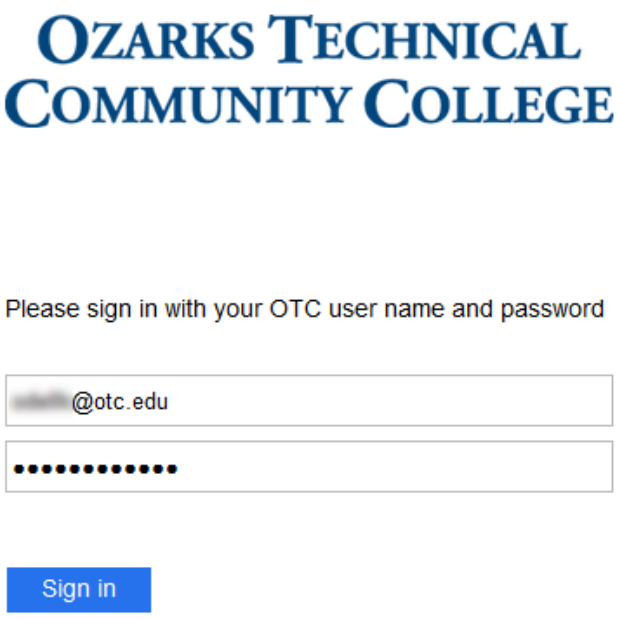
You will need a computer, the phone you will use when logging in, and your OTC username and password.

1. Go to: http://aka.ms/mfasetup

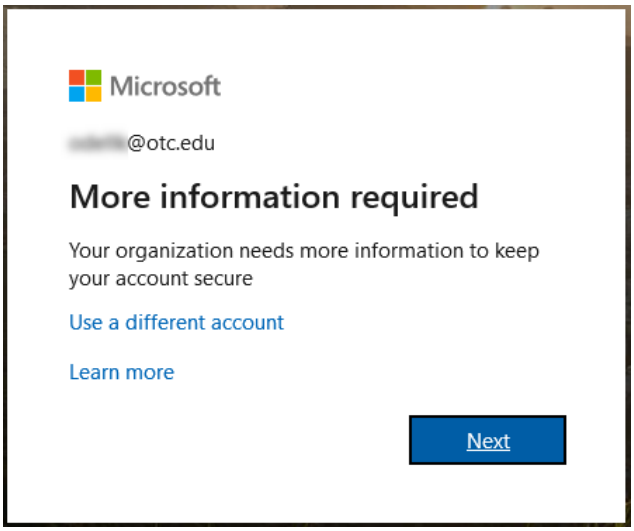
2. When prompted, enter your OTC email address.



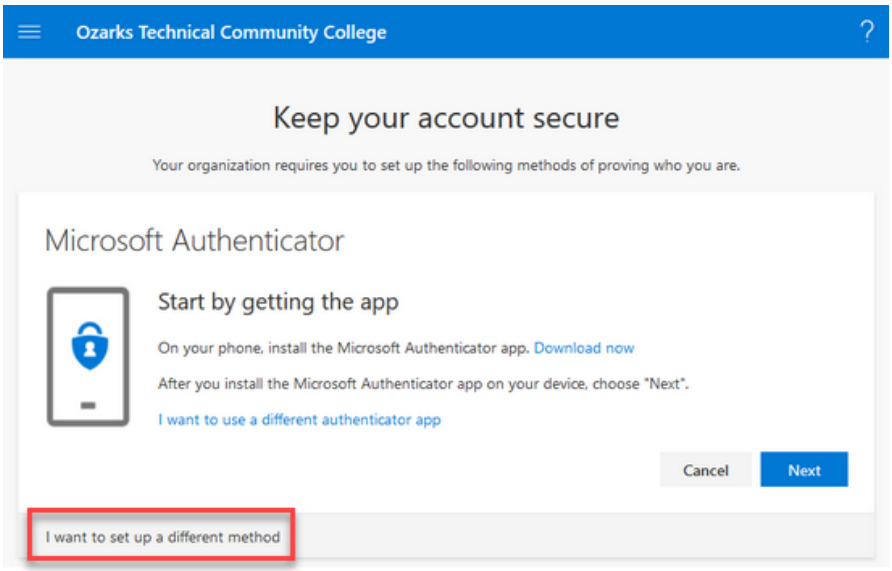
3. This will redirect you to an OTC sign-in page. **Sign in** with your OTC user name and password.



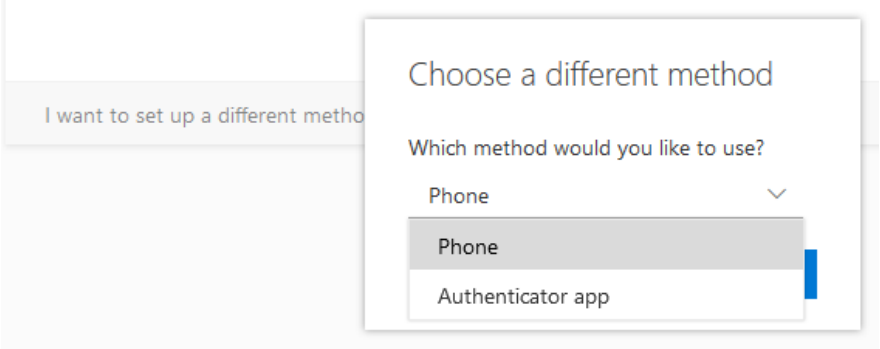
4. This will direct you to a screen which says "More information required." Click **Next**.



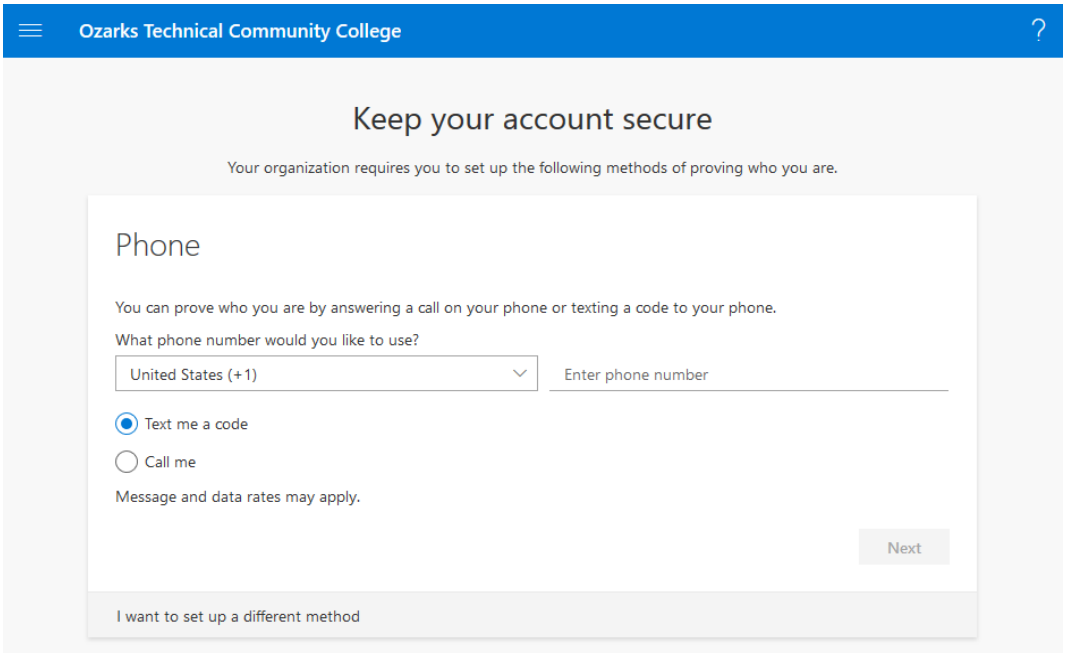
5. By default, the Microsoft Authenticator app is suggested. Click **I want to set up a different method.**



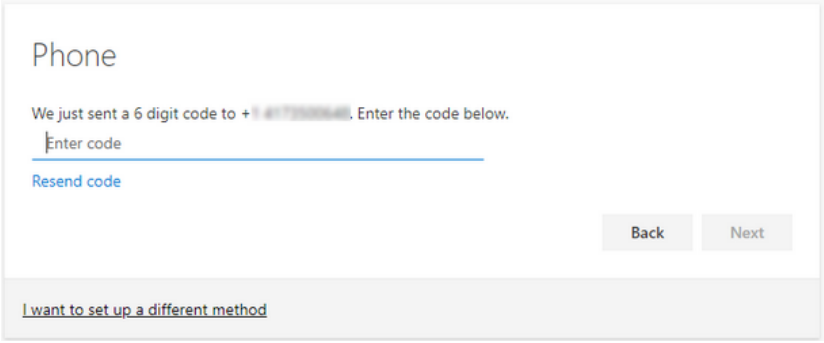
6. Select **Phone**



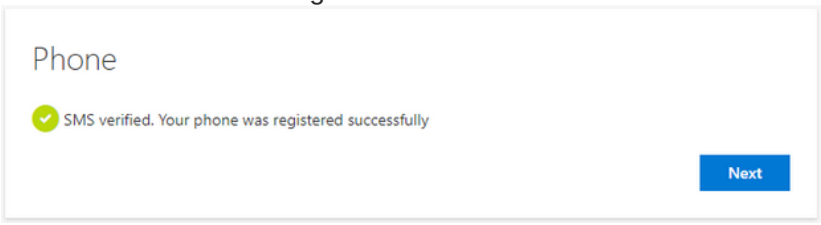
7. Enter your 10-digit phone number, and select whether you would like them to text or call, then click **Next**. (**Note:** You do not have to enter a 1 at the beginning of your phone number - this is applied automatically for you.)



8. Select the **Text me a code** radio button and click **Next**.
9. Enter the code you are given via text.



10. You will receive a message that it was verified. Click **Next.**



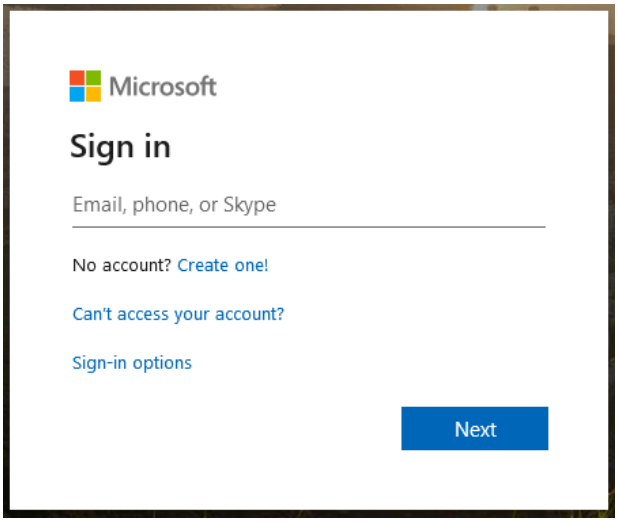
11. If all went well, you should see a screen which says "Success!" Click **Done**.

Set up your basic cell phone without SMS capabilities, or landline:

This method supports receiving a phone call for MFA verification. This method supports any smartphone, basic cell phone, or landline.

You will need a computer, the phone you will use when logging in, and your OTC username and password.

1. Go to: http://aka.ms/mfasetup
2. When prompted, enter your OTC email address.



3. This will redirect you to an OTC sign-in page. **Sign in** with your OTC user name and password.

OZARKS TECHNICAL COMMUNITY COLLEGE

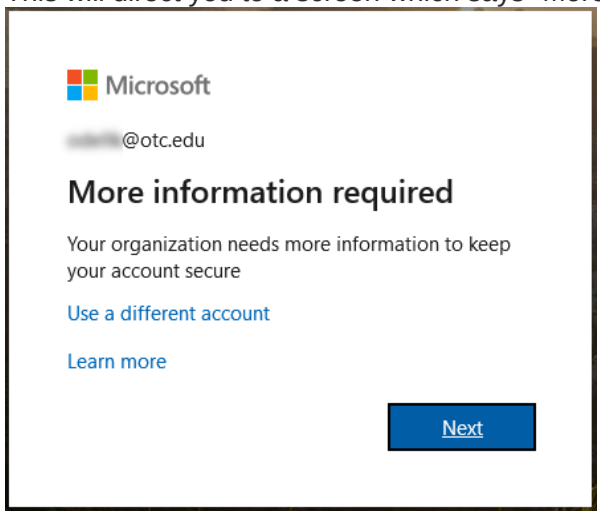
Please sign in with your OTC user name and password

[redacted]@otc.edu

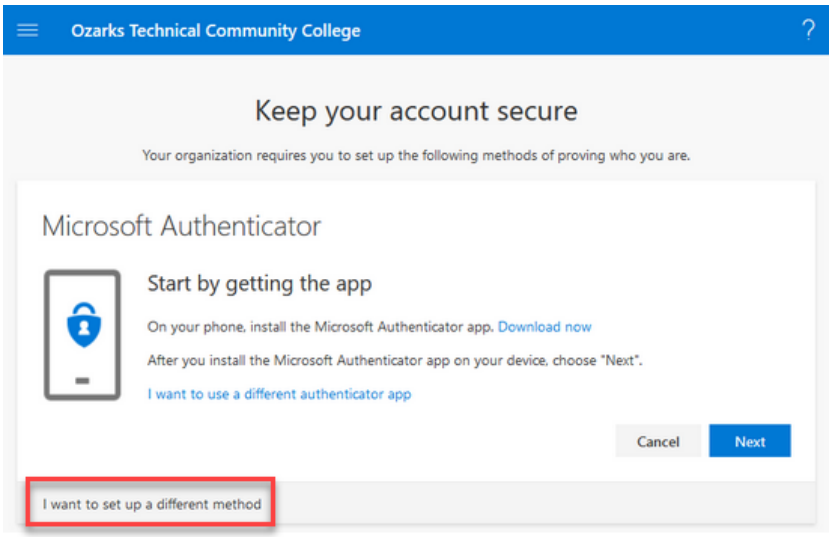
••••••••••••

Sign in

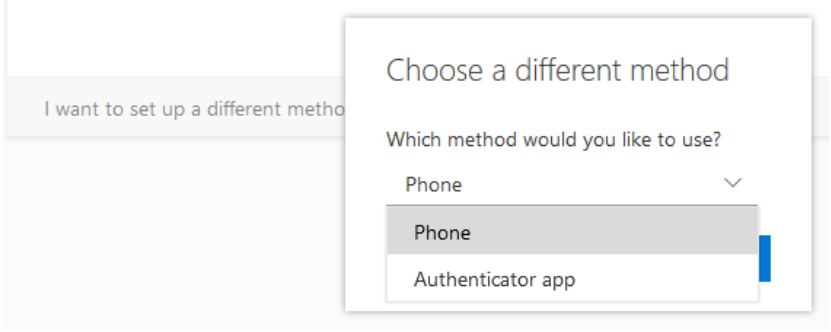
4. This will direct you to a screen which says "More information required." Click **Next**.



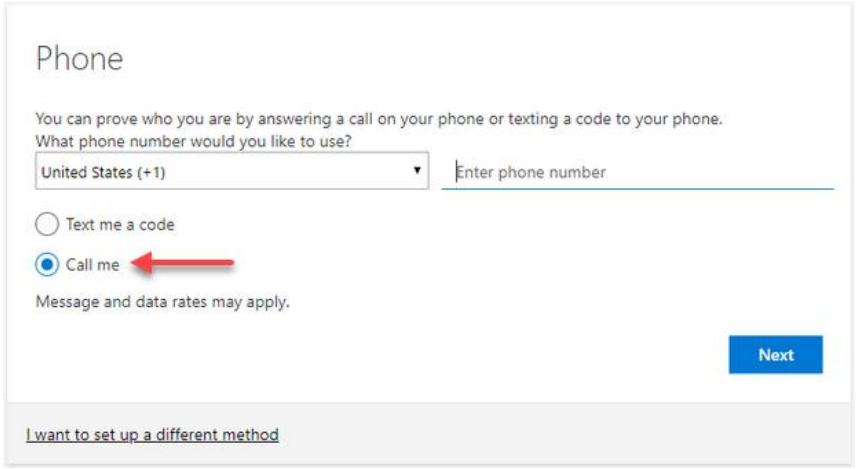
5. By default, the Microsoft Authenticator app is suggested. Click **I want to set up a different method.**



6. Select **Phone**



7. Enter your 10-digit phone number, select **Call me**, and click **Next**. (**Note:** You do not have to enter a 1 at the beginning of your phone number - this is applied automatically for you.)

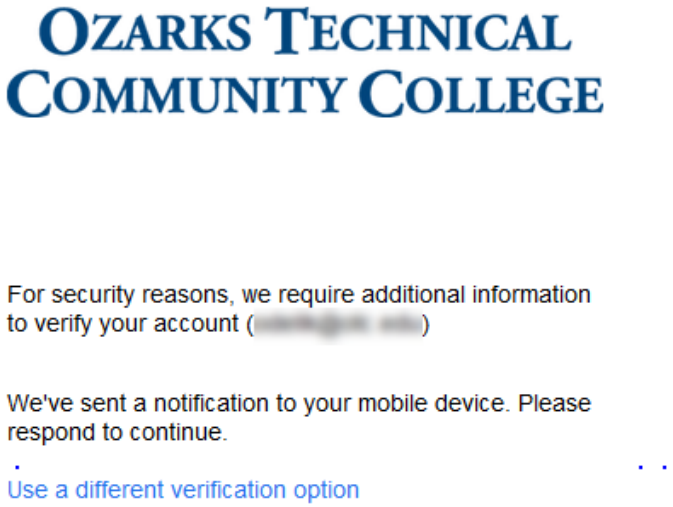


8. Answer the phone and press the # when prompted.

9. You will receive a message that it was verified. Click **Next**.
10. If all went well, you should see a screen which says "Success!" Click **Done**.

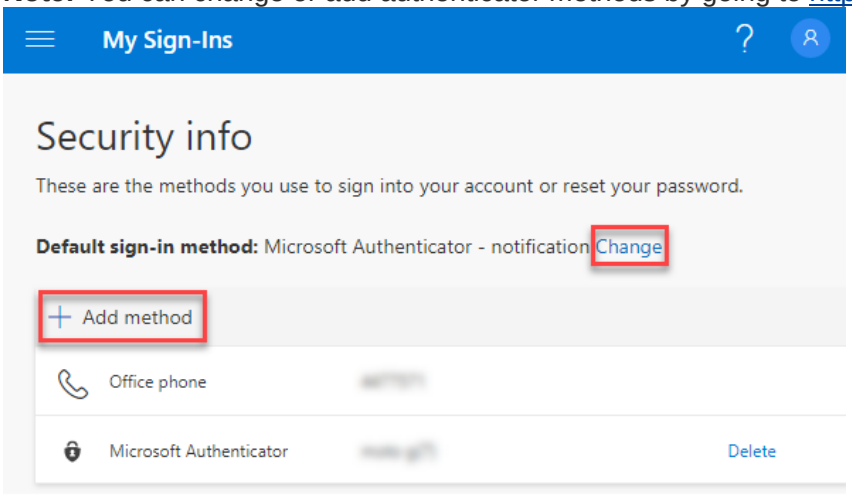
Signing in with MFA

1. Now, try to sign into any OTC service which utilizes SSO. (For example, you could go to http://portal.office.com.) Enter your OTC username and password as usual.
2. You will see a message asking for additional information:



3. Depending on the verification method you set previously, either tap **Approve** on the prompt from the app, check your text messages for a verification code, or wait for a phone call giving you a verification code.
4. You should be good to go!

Note: You can change or add authenticator methods by going to https://aka.ms/mfasetup



Frequently Asked Questions:

What is Multi-Factor Authentication (MFA)?

Multi-factor authentication (MFA) involves something you know (your username and password) and something you have (your phone). After you set up your multi-factor authentication, you will continue to use the same username and password, but you will also be prompted to provide an additional verification that you are currently trying to sign in. This extra layer of security prevents anyone but you from logging in to your account, even if they know your password. A common example would be a verification code sent via text to your cell phone when you try to log on, which you then have to enter before access is granted.

Why do I need this?

We are deploying MFA in response to a rise in the scope and sophistication of phishing and malware attacks that are targeting our faculty and staff. The high rate of successfully compromised passwords is a serious and pervasive threat to information security at OTC.

What devices are supported?

- iOS smartphones and tablets
- Android smartphones and tablets
- Blackberry devices
- Windows phones
- Basic cell phones with and without text messaging capabilities
- Landlines (desk phones)
- Hardware tokens

It is strongly recommended that you add an additional device to your MFA setup to serve as a backup.

I don’t have a smartphone, basic cell phone, landline, tablet, hardware token, or I am unable to use MFA.

If you have concerns about meeting this requirement, please contact the Help Desk at 417-447-7548.

Where can I obtain a hardware token?

You can obtain a hardware token by contacting the OTC Help Desk at 417-447-7548.

I have a YubiKey, can I use this instead of a hardware token?

Yes. Yubikeys are allowed to be use with Microsoft MFA, but they are not officially supported by OTC. You can attempt to setup you key using Yubico's official documentation.

How often do I need to use MFA?

That depends on:

- What you logged into
- Whether you're actively logged in or inactive.
- Whether the page has prompted you to always keep you sign in and you agreed to it.

In general, you should be asked to authenticate every 8 hours per browser or app on each device.

I was suddenly asked to provide MFA verification when I did not expect it. Why might that happen?

- If you sign in and out again in any MFA protected resource.
- If you change your password or have an incorrect password
- If you delete your browser's cookies or clear the browser cache.

I didn't receive the text message or the verification times out.

Delivery of SMS messages are not guaranteed because there are uncontrollable factors that might affect the reliability of the service. If you often have problems with reliably receiving text messages, please try to use the Microsoft Authenticator app or a phone call instead. The mobile app can receive push notifications both over cellular or Wi-Fi connections. In addition, the Microsoft Authenticator app can generate verification codes when the device has no signal at all.

I have lost my device or can no longer use it to perform MFA verification.

If you have set up MFA on a device that was lost, stolen, or is otherwise no longer accessible, you'll need to call the Help Desk at 417-447-7548 to verify your identity and have your Multi-Factor Authentication reset.

Once reset, you will need to set it up again using this link: https://aka.ms/mfasetup

Alternately, you will be prompted for setup through: https://portal.office.com

If you have NOT set up Multi-Factor Authentication, you may receive SAML and other authentication errors until you have completed MFA setup when trying to log into MyOTC, Canvas, the OTC Help Desk site, and other OTC resources.

Why isn't third-party email offered as a MFA verification method?

OTC is using Microsoft Multi-Factor Authentication service to provide MFA service. Microsoft does not support third-party email as a verification method for their MFA service. Microsoft's documentation website offers a list of supported authentication methods.

If I use my personal phone number for MFA, where does that phone number go? Can/will it be used for other purposes?

Phone numbers provided for MFA are stored by Microsoft. They are not used or transmitted to any other OTC service or system. See Microsoft's privacy notice for more information on their privacy policies.

Can I use MFA without a data and/or a text plan for my device?

The verification code option works with without a data plan, text plan, or even a connection. Once installed the Microsoft Authenticator App can generate a verification code without the need of either a cellular signal or data plan.

If I authenticate using my personal phone (smart or cell) will I be charged?

Charges depend on your carrier and plan, but are very nominal. The push notification is 2kb. The SMS text is standard text pricing. The phone call is the cost of a standard call. To avoid charges, you can use the Microsoft Authenticator app with verification codes.

Troubleshooting:

Smartphone General Troubleshooting

1. Restart your device
2. Verify your mobile device has a signal and internet connection. You may also try disconnecting from the WiFi network and just using a Cellular network.
3. Turn off battery optimization.
4. Additional troubleshooting steps can be found on Microsoft's Documentation.

Resetting Multi-Factor Authentication

If you have set up MFA on a device that was lost, stolen, or is otherwise no longer accessible, you'll need to call the Help Desk at 417-447-7548 to verify your identity and have your Multi-Factor Authentication reset.

Once reset, you will need to reset it up using this link: https://aka.ms/mfasetup

Alternately, you will be prompted for setup through: https://portal.office.com

SAML or other authentication errors

You may receive a SAML error or other authentication errors when trying to log into MyOTC, Canvas, the OTC Help Desk site, and other OTC resources, if:

- You have NOT set up Multi-Factor Authentication. Please follow the steps above to set up MFA using the option of your choice.

- Multi-Factor Authentication was set up incorrectly. Please call the Help Desk at 417-447-7548, and let them know the error you're receiving.
-