Multifactor Authentication Registration

Overview:
Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber-attack. A factor in authentication is a way of confirming your identity when you try to sign in. The four most common kinds of factors are:

- Something you know - Like a password, or a memorized PIN.
- Something you have - Like a smartphone, or a secure USB key.
- Something you are - Like a fingerprint, or facial recognition.
- Somewhere you are – Like your geolocation, or IP address.

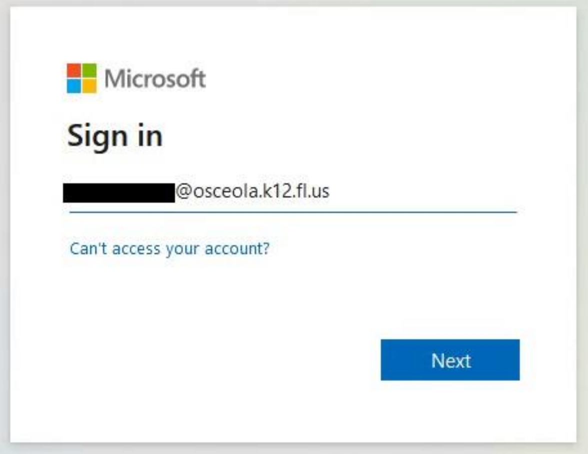
MFA is designed to ensure you are the only one who can access your account — even if someone knows your password. MFA is a proven and effective way to protect against many security threats that target passwords, such as phishing. MFA is a 2-step verification process that requires the use of more than one verification method whenever you are accessing district resources (e-mail, TEAMS, OneDrive, etc.) while away from campus.

For more information, you may visit the following Microsoft articles:
- Multifactor Authentication First Time Setup
- Manage Your Security Info

Registration:

To help protect our Office 365 accounts, staff can setup additional verification options to help better secure their accounts and resources. Please follow the following steps to register for multifactor authentication.

1. Open a web browser and navigate to your **My Account** page by visiting: https://myaccount.microsoft.com
2. Staff will sign in with their @osceola.k12.fl.us email:



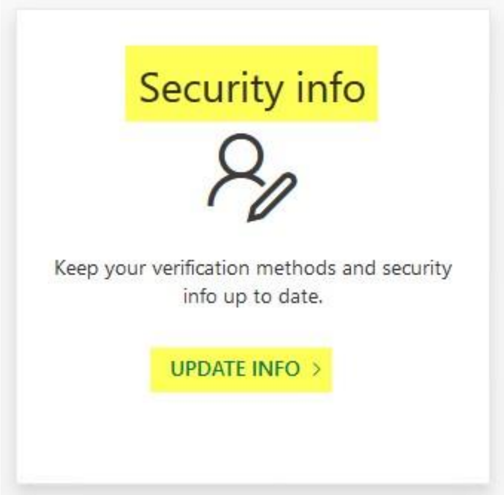
Microsoft

Sign in

[redacted]@osceola.k12.fl.us

Can't access your account?

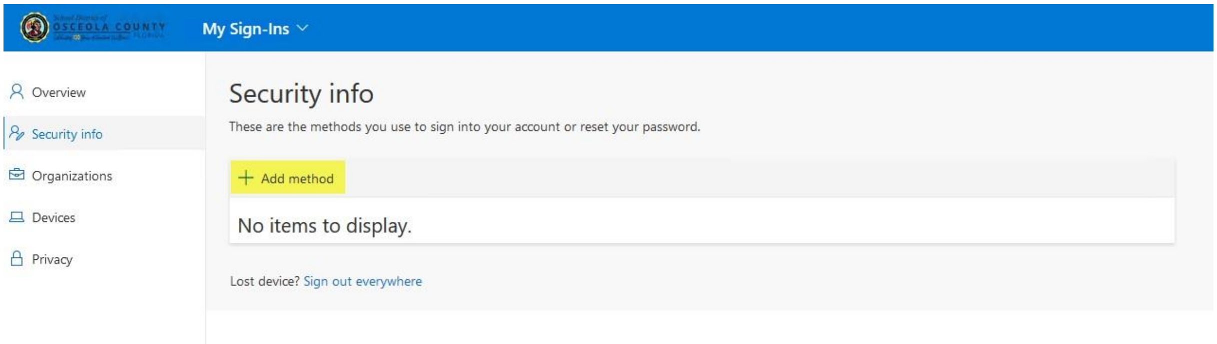
3. Navigate and click on "Security Info" on the left pane.



Security info

Keep your verification methods and security info up to date.

4. Under Security Info, select **+ Add method**:



Security info

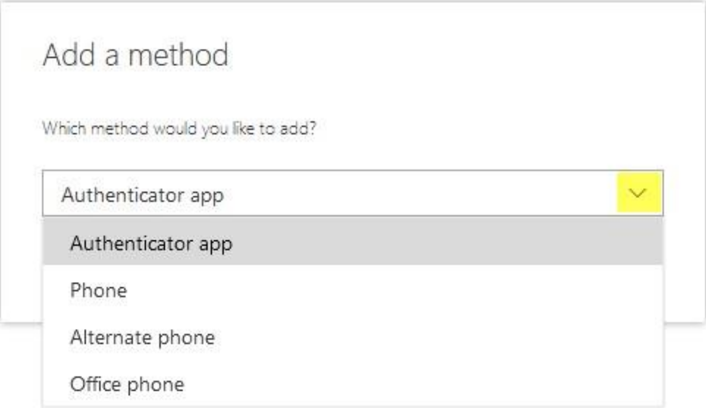
These are the methods you use to sign into your account or reset your password.

No items to display.

Lost device? Sign out everywhere

5. Click on the drop-down arrow in the “Add a method” window to select your preferred method to authenticate.

   Please note: The wording may vary slightly as Microsoft updates the options, but the general instructions apply.

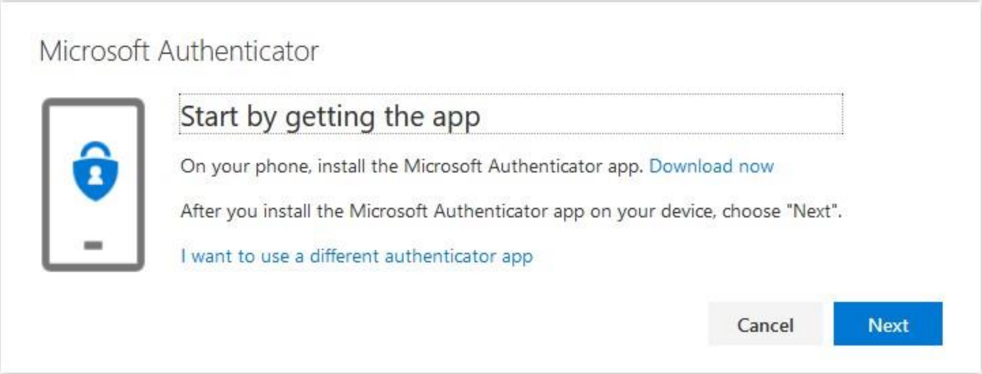


Add a method

Which method would you like to add?

6. There are multiple Authentication options available to choose for Multifactor Authentication:

   A. Authenticator App – Microsoft Authenticator, Google Authenticator, etc. (Most secure)



Microsoft Authenticator

Start by getting the app

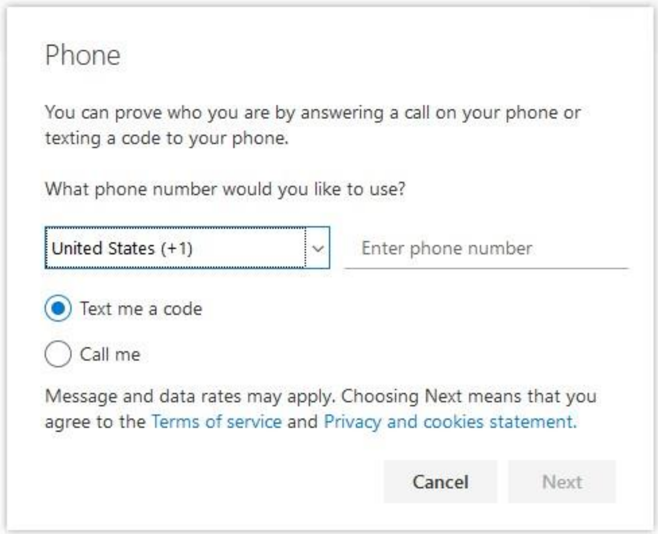
On your phone, install the Microsoft Authenticator app. Download now

After you install the Microsoft Authenticator app on your device, choose "Next".

I want to use a different authenticator app

Using your smartphone, you may download the Microsoft Authenticator app from the Google Play store for Android devices or App Store for Apple iOS devices. Alternatively, you may also choose to use a different authenticator app. For either case, follow the remaining steps to complete the setup of your chosen authenticator app.

B. Phone – This is your Primary Phone option to receive a call or code sent through Text Message (SMS).



Phone

You can prove who you are by answering a call on your phone or texting a code to your phone.

What phone number would you like to use?

United States (+1) | Enter phone number

● Text me a code

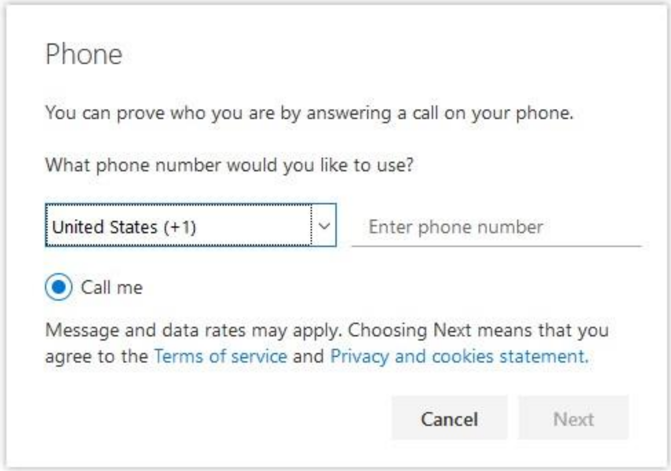
○ Call me

Message and data rates may apply. Choosing Next means that you agree to the Terms of service and Privacy and cookies statement.

For the “Text me a code” option, which is only available on the primary phone, you will receive a text message with a code to enter to complete the setup process.

For the “Call me” option, you will receive a call from a Toll-Free number and it will guide you through the rest of the setup process.

C. Alternate Phone/Office Phone – Phone Call Verification Only, No Text Message Option



Phone

You can prove who you are by answering a call on your phone.

What phone number would you like to use?

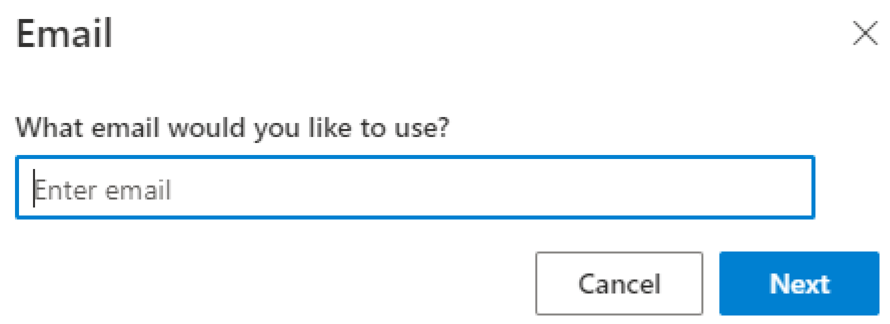
United States (+1) | Enter phone number

● Call me

Message and data rates may apply. Choosing Next means that you agree to the Terms of service and Privacy and cookies statement.

Similar to the previous section, for the “Call me” option, you will receive a call from a Toll-Free number that will guide you through the rest of the setup process.

D. Email (Not recommended for better security)



Email

What email would you like to use?

You may enter another email address (non-district) to receive a code. You will then provide this code to sign-in to your Office products. This method is not recommended because it is not a second factor of authentication - both are “Something you know.” An attacker who has access to one of your accounts may have access to multiple accounts.

This concludes the overview and instructions for registering for Multifactor Authentication.