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:

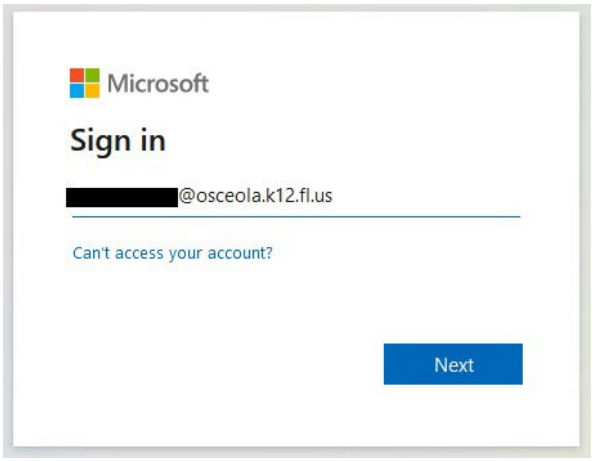
- Multifactor Authentication First Time Setup
- Manage Your Security Info

Registration:

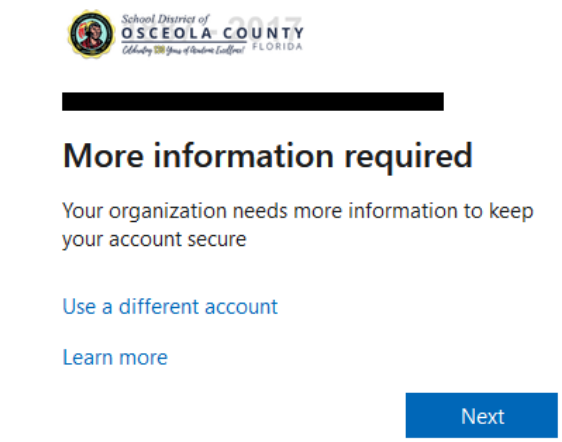
To help protect our Office 365 accounts, staff are required to setup additional verification options to help better secure their accounts and resources. Please follow the following steps to register for multifactor authentication.

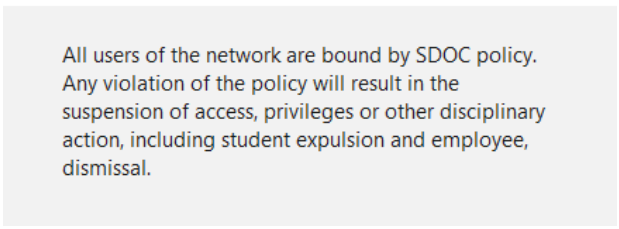
1. Open a web browser and navigate to your **My Account** page by visiting: https://myaccount.microsoft.com

2. Staff will sign in with their @osceola.k12.fl.us email:

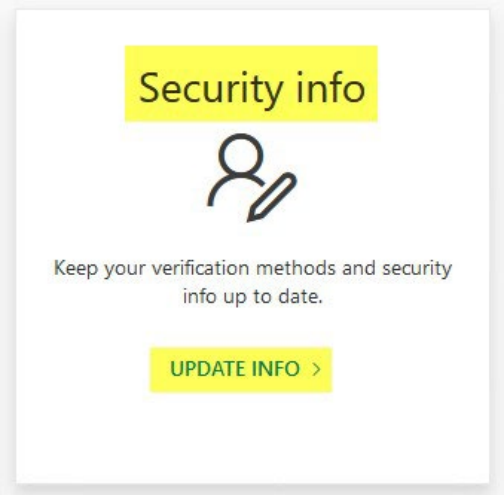


3. You may be prompted to provide additional details if you have not already registered for multifactor authentication (MFA):

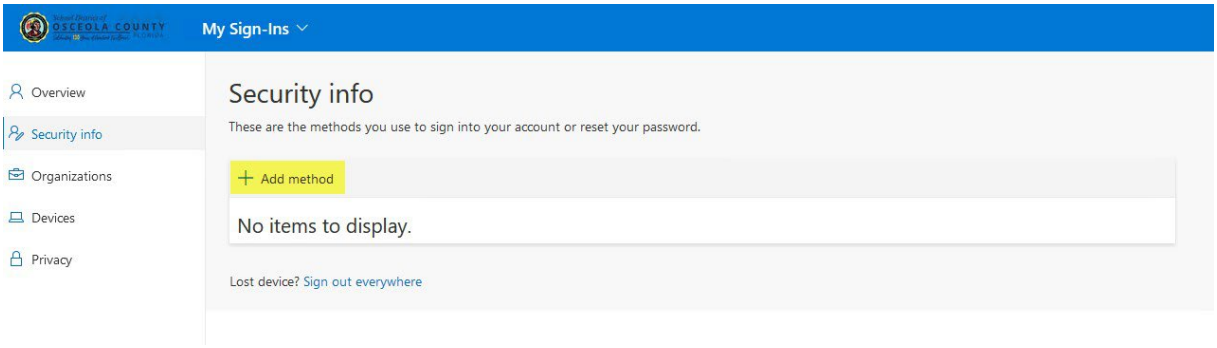




4. Once logged-in, navigate and click on “Security Info” on the left pane.

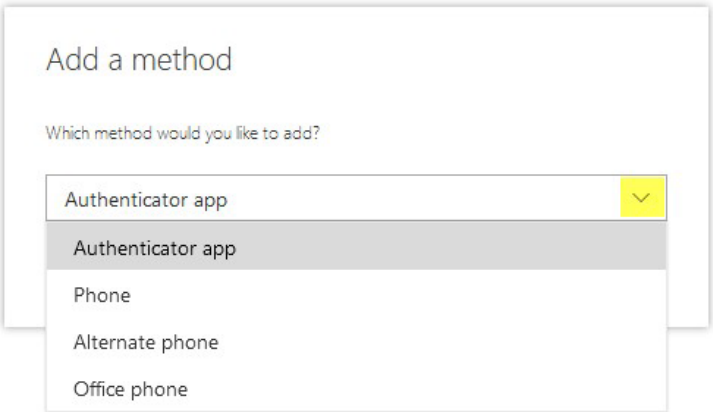


5. Under Security Info, select **+ Add method**:



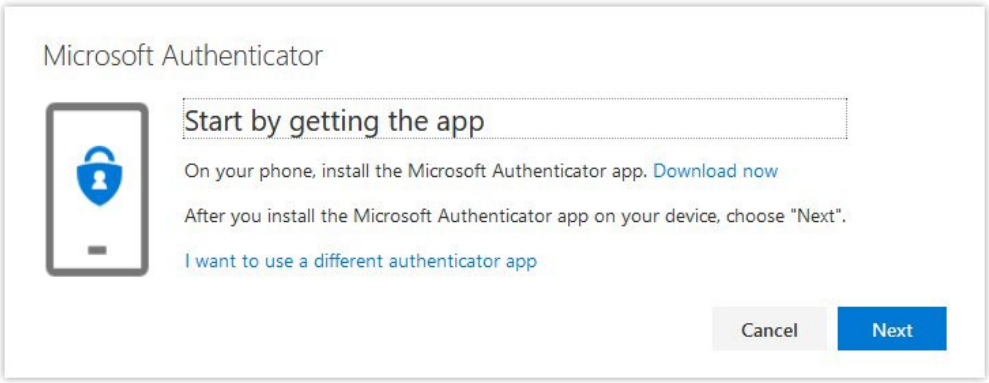
6. Click on the drop-down arrow in the “Add a method” window to select your preferred method to authenticate.

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



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

   A. Authenticator App – Microsoft Authenticator, Google Authenticator, etc. (**This is the most secure and recommended option**).

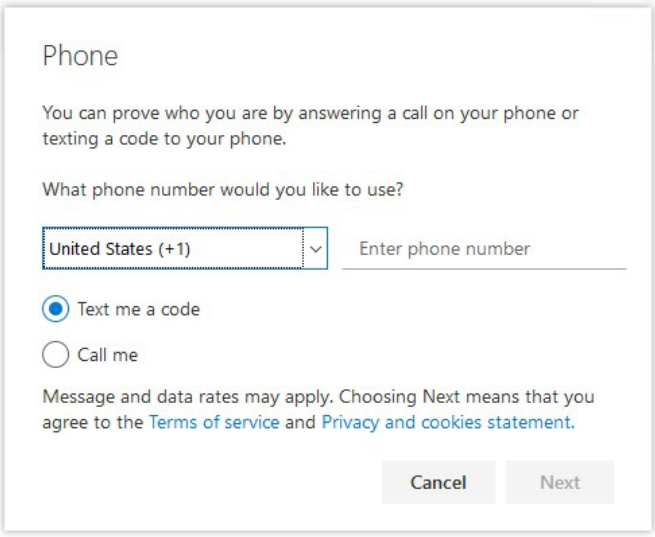


Using your smartphone, you may download the Microsoft Authenticator app from the Google Play store for Android devices or App Store for Apple iOS devices.

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.

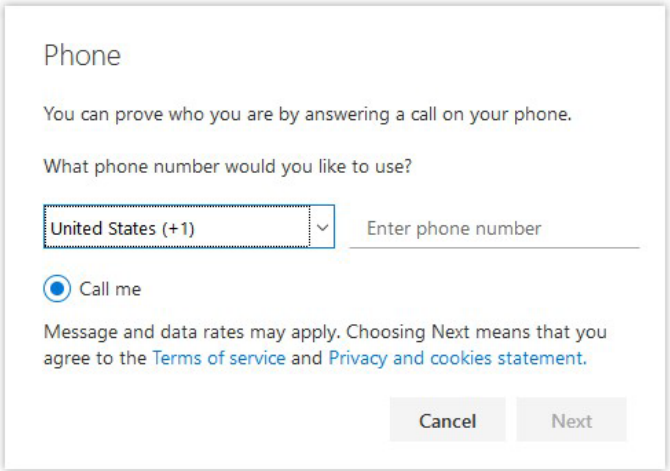
B. Phone – This is your Primary Phone option to receive a call or code sent through Text Message (SMS).



i. 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.

ii. For the "Call me" option, you will receive a call from a Toll-Free number, which will guide you through the rest of the setup process.

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



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

Note: It is not recommended to use your Office Phone for MFA. If you are accessing resources from outside the office, you will not be able to answer your office phone.

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