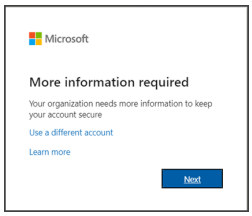
Office365 Multi-Factor Authentication (MFA) Procedure

Multi-Factor Authentication (MFA) is the most effective way to protect your Microsoft Office 365 account from malicious sign-ins. MFA works by requiring something you know (like a password) AND something you have (like a phone). MFA will prompt you to enter a unique 6-digit verification code sent via SMS text/phone call or approved through the Microsoft Authenticator App. Without being able to provide that "second factor" malicious actors cannot sign into an account to steal data or send phishing messages. The following are the steps to set up MFA.

1. The Information Technology Division (IT) enforces MFA for your Microsoft O365 account
2. Sign into your account with your password, like you normally do. After you choose "**Sign in"**, you will be prompted for more information.



4. Choose **Next**.
5. The **default** authentication method is to use the free Microsoft Authenticator app. If you have it installed on your mobile device, select **Next** and follow the prompts to add this account.
6. To get the application on your phone, you can scan the QR codes provided below for your Android or IOS mobile device.

Microsoft Authenticator

It is highly recommended (but not required) for you to use the Microsoft Authenticator app.

*Instead of the recommended Microsoft Authenticator App, to verify your identity via SMS messages sent to your phone, select **"I want to set up a different method",** then provide your mobile number. The system will text a 6-digit code to verify your device. If you don't have a cell and choose to use your Office phone, it is recommended to add an Alternate phone so when you are logging in away from that landline and not able to accept a verification call, the system has a way to reach you to complete the login. You may add multiple MFA Methods and use any one of them at time of login.*

After successfully logging into O365, you can edit your MFA options anytime at the following address: https://myaccount.microsoft.com/> Under Security info hit Update Info > +Add Method.*

*If you are planning to change the phone number chosen for MFA, or getting a new cell phone, prior to loosing access to that number/device, add an additional method. You can have multiple MFA methods and remove old numbers/devices.

7. Whenever you sign into Microsoft 365 from a new location and at regular intervals, you'll be prompted to provide the additional verification information or action, such as typing the verification code provided via text/phone-call or completing an approval through your authenticator app. ***Each application (Outlook, Teams, SharePoint) will prompt, it is normal to get multiple MFA prompts during a verification interval***.

Protection information: If you receive an unexpected MFA verification text or authenticator app approval request (unexpected as in you are not on a device awaiting MFA entry), **DENY** the MFA prompt on the authenticator app and **immediately change your password** through Clever: https://sso.browardschools.com (top right corner, click on your name, "**Change AD Password**" dropdown).