Multi Factor Authentication FAQs

What is Multi-Factor Authentication (MFA)?

- Multi-Factor Authentication (MFA) refers to an additional layer of security that is added to the login process.
- MFA relies on two forms of authentication: something you know, and something you have with you. The something you know is your password. The something you have with you can be a mobile device. This means that even if your password is hacked, your account will remain secure.
- Learn more about Microsoft’s Multi-Factor Authentication on the Microsoft Overview Page.

How often do I have to re-authenticate?

- The current settings require reauthentication every 14 days (if box is checked) OR with EACH login if you have a Microsoft administrator account.
- You will need to re-authenticate on each device and each browser you use.

What are my authentication options?

- You will be able to choose a primary authentication method when you register, which you can change or update at any time.
- Current options are outlined below:

<table>
<thead>
<tr>
<th>Verification Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Notification (Microsoft Authenticator Required)</td>
<td>A push notification is sent to the Authenticator app on your smartphone asking you to authenticate your log in. (This option is recommended for international users)</td>
</tr>
<tr>
<td>Verification Code (Authenticator apps available in App Store/Play Store)</td>
<td>The authenticator app will generate a verification code that updates every 30 seconds. You will be asked to enter the most current verification code in the sign-in screen.</td>
</tr>
<tr>
<td>Text Messages</td>
<td>A text message with a 6-digit code is sent to your mobile device that you will input to complete the authentication process.</td>
</tr>
<tr>
<td>Phone Calls</td>
<td>A call is placed to your mobile phone asking you to verify you are signing in. Press the # key to complete the authentication process.</td>
</tr>
</tbody>
</table>

- You will also be asked to set up a backup authentication method. ITS recommends that you use your office phone as a backup, to help you access your account in case you forget or lose your mobile device.
How do I set up the Microsoft Authenticator App (Azure) on my phone?

- Use our MFA First Time Set Up Guide or watch the Microsoft video on How to register for Azure Multi-Factor Authentication. For questions regarding the Microsoft Authenticator App, please refer the Microsoft Authenticator page.

How do I change or update my authentication method?

- You can make changes to your authentication settings by visiting the Microsoft Security Verification page. For instructions follow our MFA First Time Set Up Guide.

Can I use my Personal Device to set-up MFA?

- Yes, IT encourages the use of a personal device for MFA.

What if I experience issues with MFA?

- You can contact the Help Desk at helpdesk@nycc.edu or 315-568-3911 or review Microsoft’s MFA Troubleshooting Page.