Preparing for Office365 Multifactor Authentication (MFA)

Things to Know and Prep Work

- If you are running an older version of Office 365, please update today, MFA is supported on 2013 version and up. The most current version is available on Software Center and Company Portal while on the BCPS network.:
  - Note: If you have an older Office version, and find issues once MFA is enabled, please go through https://sso.browardschools.com to use the online O365 until you can upgrade Office to a compatible version.
- If you are accessing email on your cell, please make sure you are using the Outlook app (not a third-party email client)
- While it is preferred and easiest to use the Microsoft Authenticator app or SMS text, we understand some may not be comfortable using their cell phone. In this case, you may also use a land line as your first MFA option however, you would need to add an option that follows you so that if you ever log in away from that landline you will still have an alternate way to request the second factor be delivered – either through SMS or Authenticator app.
- You can edit your MFA options anytime here:
  https://myaccount.microsoft.com/ > Under Security info hit Update Info > +Add Method
- Each app may prompt for an MFA approval individually, so if you use Outlook, Teams, Word, and MS Planner, expect to get multiple MFA prompts, one for each item at Windows login, new browser session, new app use, when you connect from a different physical location. There is a time when MFA will be cached, and randomized intervals of use allowed before being prompted again. Rest assured, if an attacker tries to use your account – it is likely that they will do so from a new physical location and therefore always get prompted and because they will not have that second factor to enter… they will not be able to get in, even if they know your password.
- If you have automatic jobs on O365 related tools like PowerAutomate or Microsoft Flow, once MFA is enabled, be prepared to be prompted for a second factor for each item individually. It is normal to have many MFA approvals, one for each tool or app.
- Multifactor is used to prevent an attacker with your user and password from being able to get in because they will not be able to enter the MFA digits or have the authenticator app authorized to approve the request. If you ever get an **unexpected MFA prompt**– as in, you are not actively trying to log in, **DENY the MFA prompt**. MFA is pushed only when you are interacting with your device and see that device asking for approval. If you get prompted 'out of the blue', it could be an attacker and you should change your password.
- This document is prep for accompanying file "O365 Multifactor MFA Procedure.pdf" where we walk you through the process, don't worry, it's not that bad and totally worth the protection you get!