Enabling 2FA is now a required step in ensuring that the College is following the latest security best practices while remaining in compliance. Here at Southwestern, and especially in IT Services, we take data privacy very seriously. A lot of personal information is required to make the College go 'round, and it's our responsibility to ensure that that information is protected from prying eyes and ears.

Getting set up:

- There are multiple ways to set up your 2FA -- you can download an authenticator app such as Microsoft Authenticator on your mobile device (click here for Apple Devices, Android Devices) ***This is the recommended method as it allows you to login anywhere quickly and requires only Wifi to use, especially for Faculty and those who use multiple workstations***.
- You can also choose to set it up using a personal mobile phone number (for either text or phone call) or office phone number (the limitation of using your office phone is that it is stationary while you are not and will pose problematic when authenticating on a computer away from your desk).
- All of these options will pop up as options when you login to your Office 365 or any school related applications such as Canvas.
- If you do not want to use your personal mobile device, please let us know and we will work to figure out alternative options **Note: utilizing an authentication app or personal phone number for authentication does not constitute use for work purposes and will not jeopardize the security or privacy of your personal device.

Helpful Infobits:

- In general, once you've authenticated your account, you should not have to do so again for 90 days, this is automatic and does not need to be selected.
- If you "Log out" or "Log Off" Microsoft manually, you will be asked to authenticate upon next login. (This refers to your Microsoft 365 account, not the computer itself).
- In the case of classroom computers Faculty should only need to authenticate once per computer per day, but it could be more if the computer restarts (Classroom computers are set to clear all settings every 24hours or upon restart).
- If you login using another web browser or login on another computer, you will be prompted to authenticate again even in this 90 day window. This is to make sure that the person logging in on the new device is actually you and not someone trying to hack into your accounts from another computer.
- Once you authenticate on your browser, you will no longer need to authenticate multiple applications accessed from that browser. Example: If I log into SharePoint and authenticate on the Edge web browser and I navigate to Canvas or my Office 365 it will automatically log me in. This means fewer individual logins.
- Your chosen web browser will save your information via cookies, if you clear your cookies from your browser you will need to reauthenticate. The use of Private or Incognito windows will require authentication each time.
- Personal devices: 3rd party Browser extensions have been known to cause issues with repeated authentications. Try disabling them or whitelist the Microsoft login sites and sso.socc.edu sites in the extension. (If you're not sure what this means, it probably isn't something you use 😉)
- Desktop applications such as TEAMs and Outlook etc., are separate from your web browser so you may have to authenticate these individually. Once authenticated these also have a 90 window before prompting to authenticate again.
- 2FA allows us to be compliant on the Cybersecurity portion of our insurance, it is now required. We are audited on this.

We want to thank you again for all of your cooperation, and for reporting issues and taking the time to provide the feedback that allows us to thoroughly troubleshoot issues as they come up. Remember, 2FA means if hackers steal your NetID and password, 2FA will help protect your Campus email, Office 365 account, Canvas and all other SWOCC associated apps. With 2FA, you guard your account with both your password and your selected authorization method (App, phone # etc) to keep our data secure.

For an example of what can happen when an institution isn't properly prepared and what the consequences of a successful cyberattack can be to a rural college, check out this article published recently in Forbes (Cyberattack Article). With colleges being the most frequent targets of cyberattacks, we take SWOCC's cybersecurity very seriously and if we all work together, we can mitigate the risks to everyone. If you are experiencing any issues, or need assistance, please file ahelpDesk ticket (here), or call our HelpDesk line at 541-888-7999. (This information will also be available on mLL on the IT Help tab).