# Microsoft 365 Multi-Factor Authentication (MFA) & Self-Service Password Reset (SSPR) Registration Guide

FOR TAYLOR'S GROUP AND HIGHER EDUCATION

ICT, TAYLOR'S UNIVERSITY
EMAIL: TLSC.ICTServiceDesk@taylors.edu.my | URL: https://servicedesk.taylors.edu.my/

# Contents

# Purpose

This Registration Guide is intended to serve as a How-To document for registration to the **Multi-Factor Authentication (MFA)** and **Self-Service Password Reset (SSPR)** features, which are designed to add more security to your online credentials, i.e. Office 365 account.

# Introduction

**Multi-Factor Authentication**, also referred to as two-factor verification, is an additional verification step to help protect your online credentials. It consists of a combination of your username, password, and a mobile device or phone.

Multi-factor verification is more secure than just a password because it relies on two forms of authentication:

- Something you know, like your password.
- Something you have, like a phone or other device that you carry.

Multi-factor verification can help stop malicious hackers from pretending to be you. Even if they have your password, the odds are that they do not have your device, too.

The **Self-Service Password Reset** (SSPR) feature, on the other hand, gives you the ability to change or reset your password, with no administrator or help desk involvement. If your account is locked or you forgot your password, you can follow prompts to unblock yourself and get back to work. This ability reduces help desk calls and loss of productivity when you cannot sign on to your device or an application.

Both MFA and SSPR are enabled through a **combined registration process**, in which you can register once and get the benefits of both MFA and SSPR. What follows is a simple step-by-step guide on how to complete this combined registration process.

**NOTES**:

1. Registration requires the chosen **authentication device to be functional** to complete the registration.

2. You should only use your **personal mobile number** for MFA and SSPR registration.

3. MFA requires the user's awareness when they have made a request for authentication. Meaning the user has the option of denying the authorization if they did not submit the request themselves. A user must be aware if they **deny three (3) consecutive authentication challenges**, their account will go into a **short lockout period** and will be unable to access Office 365 resources for a few minutes. Once released from the lockout, any further consecutive denials will result in progressively longer lockout periods. This is important as an unprovoked authentication challenge could mean that the user's credentials have been compromised and malicious actors are attempting to access the account from outside the Taylor's network. Anytime this occurs, user should **immediately change their password** and **inform ICT** staff of the incident.

4. A user can "miss" (or not answer) **three (3) MFA challenges before the account locks**. After **15 minutes**, the account will automatically be re-enabled.

5. If you are not expecting an authentication prompt, you can decline the authentication:
   - By app: Press **Decline** upon receiving the notification.
   - By text message: OTP times out after **5 minutes**, after which the authentication is denied.
   - Microsoft Authenticator: App generates a new OATH verification code **every 30 seconds**.

# One Time Registration for MFA and SSPR

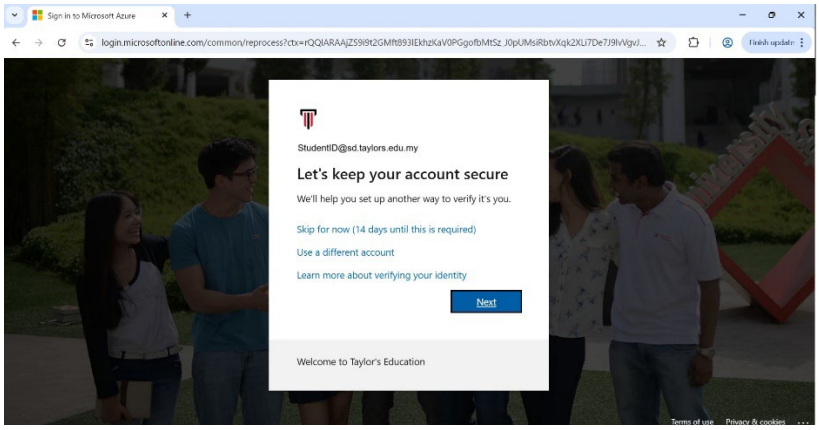
**Note:** Before you start, please ensure that you have downloaded the **Microsoft Authenticator app** on your phone from Google Play or Apple App Store.

## 1. To access Registration Page

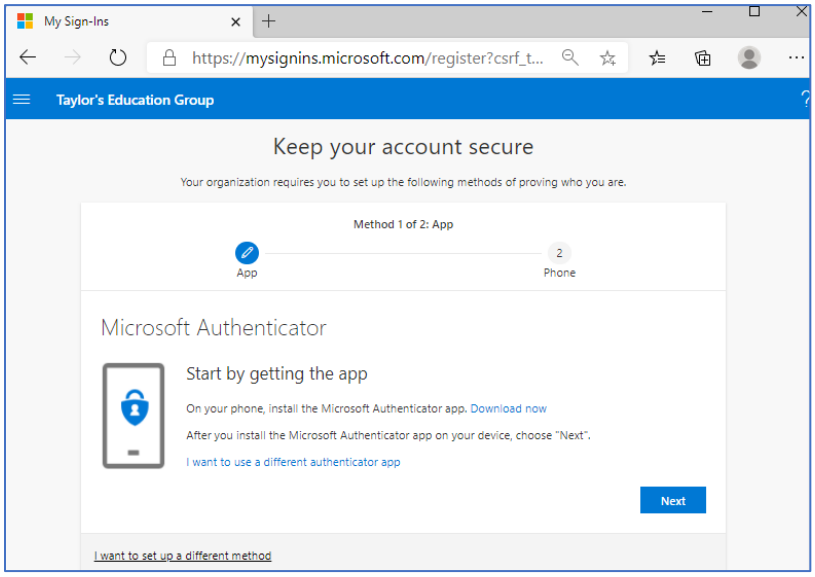
a. Open the following URL in a web browser: https://aka.ms/MFASetup
b. Enter your Taylor's Office 365 **student** email address and password.
c. Click **Sign in**

## 2. To begin registration on your Computer

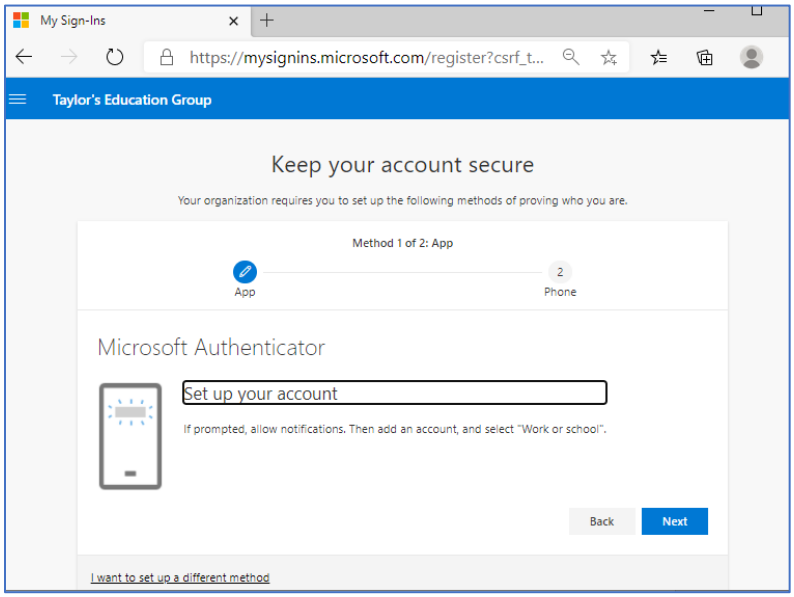
a. Select **Next** to begin the registration process.




b. In the following page, you should see the new sign-up page. Click **Next**.




c. Proceed to click **Next**. Do ensure you have **downloaded the Microsoft Authenticator** on your phone.



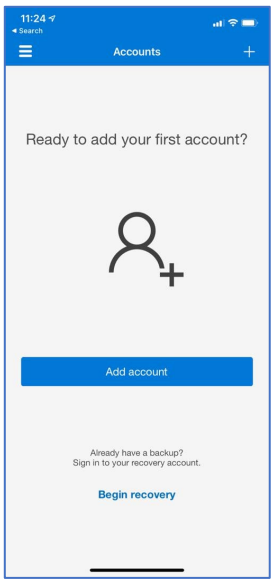

## 3. Register the Microsoft Authenticator App for MFA

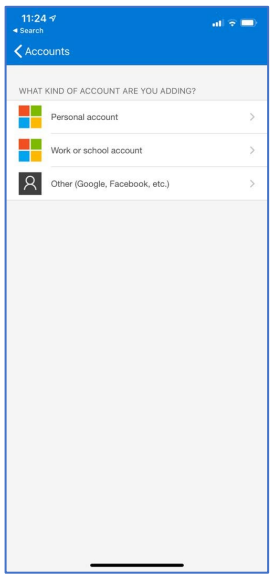
a. Open the **Authenticator App** on your phone.

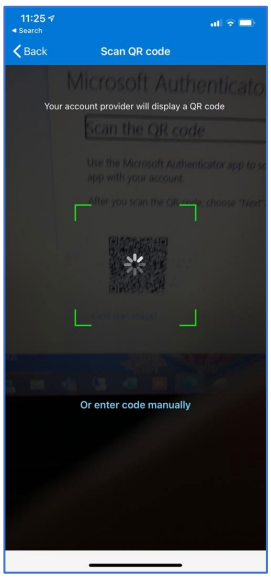
b. Click on **Add account**, even if your account is listed.

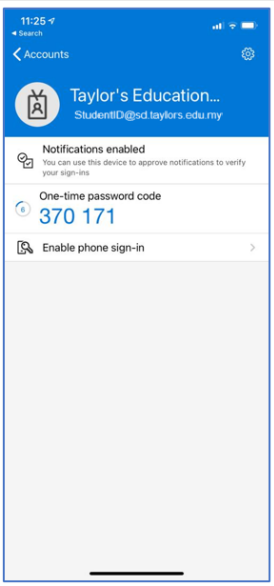
c. Select **Work or school account**.

d. **Allow** the Authenticator app to access your camera when requested.

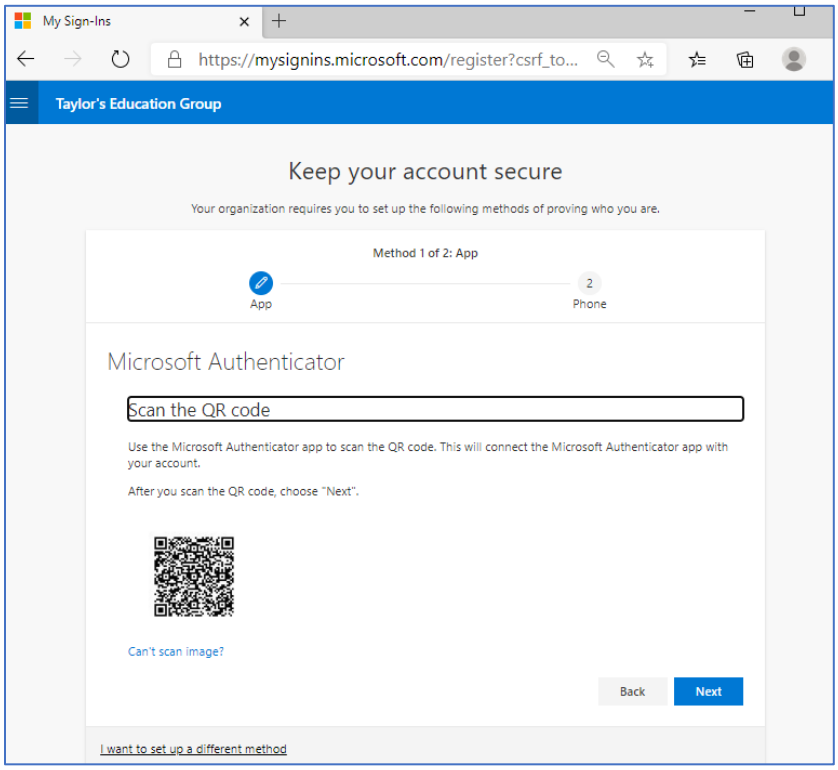


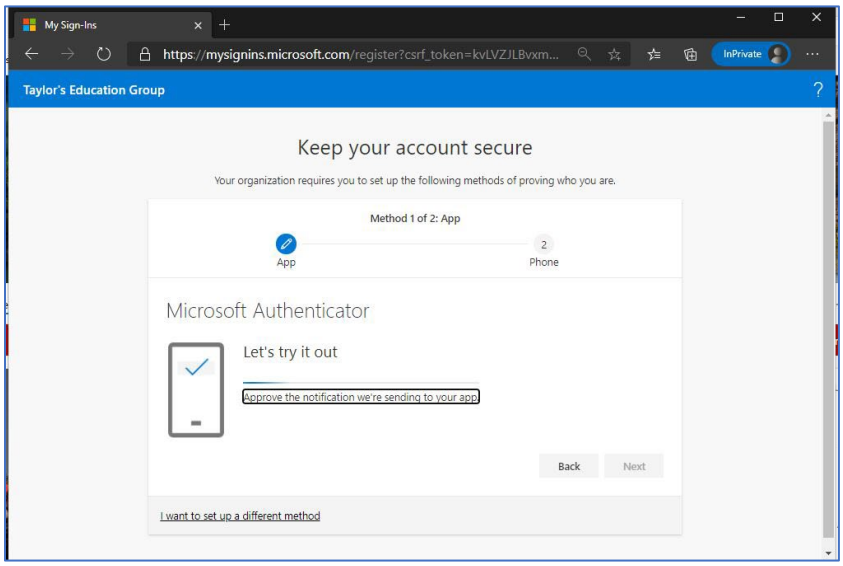



e. Return to your computer at this juncture. Scan the **QR code** on the registration page. This will auto configure your profile on the Authenticator app.

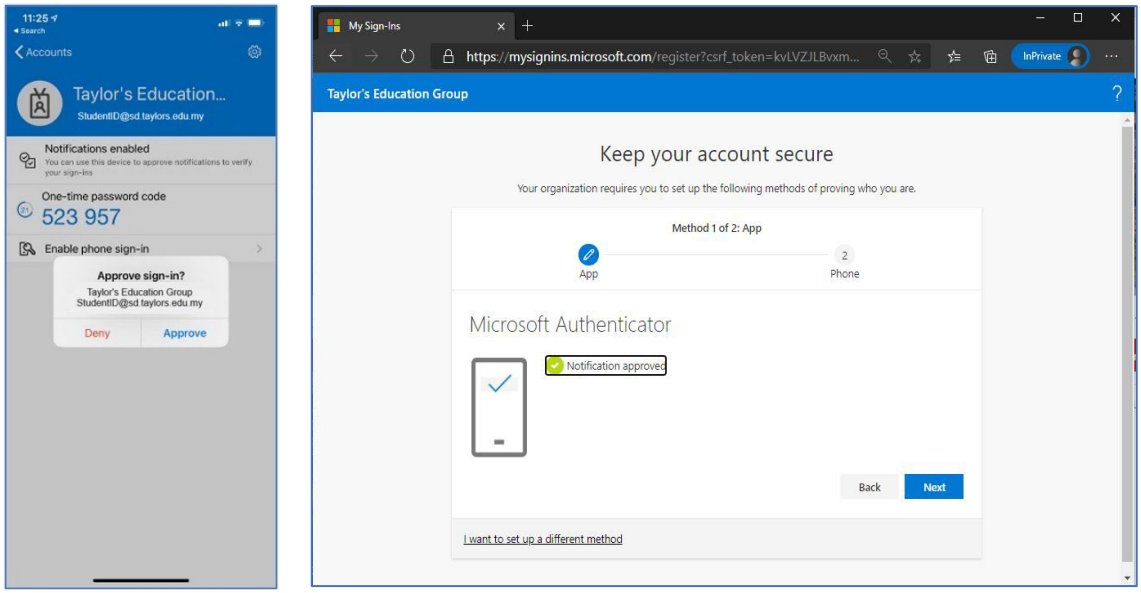


f. Click **Next** on your computer.

g. With your Authenticator app configured, the registration page would send a test request to the app.




h. You should see a prompt on the Authenticator app for an approval. Click **Approve.**

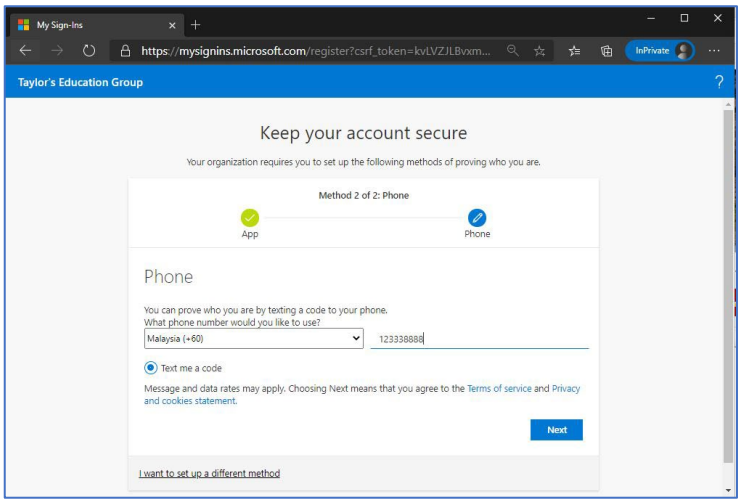


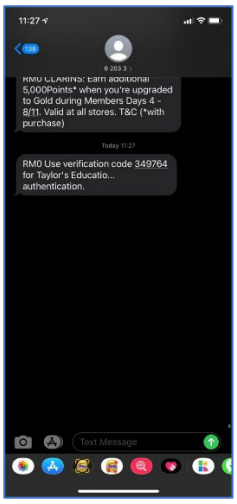

i. This completes your Authenticator app registration to your account. Click **Next** to resume with Phone registration.

## 4. Register your Phone for MFA

a. On the next screen, you will be asked to update your phone number as an alternate method for MFA.

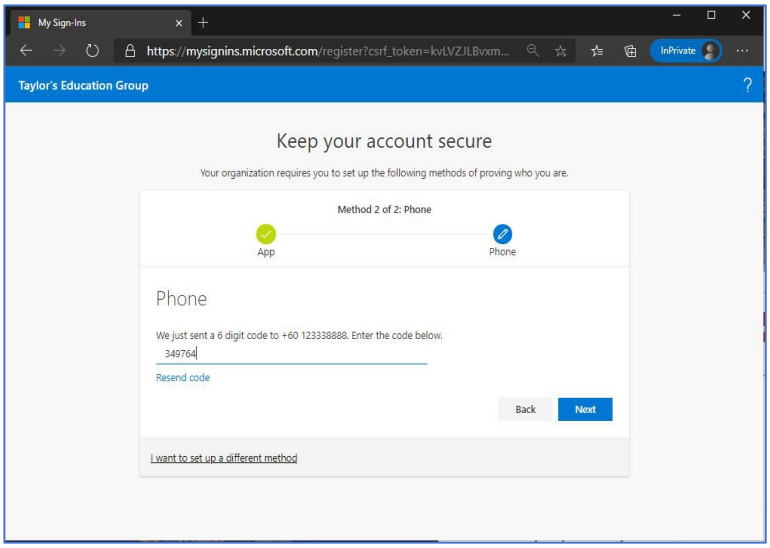
b. Enter your mobile number and click the **Next** button. Your phone will receive a 6-digit SMS verification code.

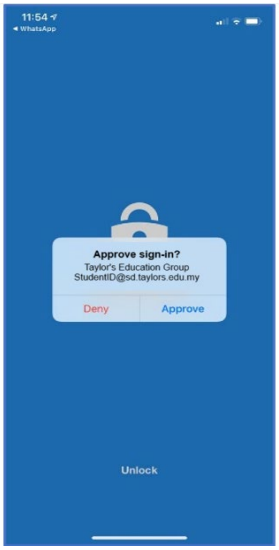


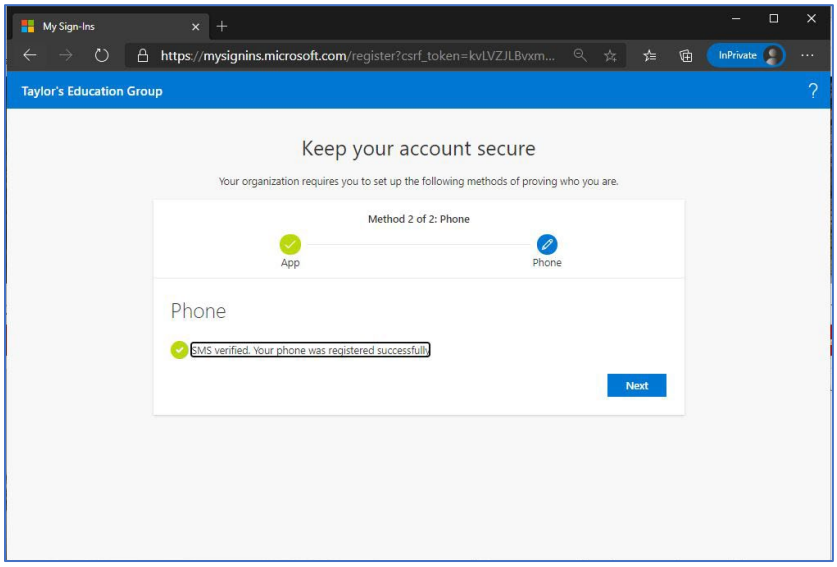

c. Enter **verification code** from the text message sent by Microsoft. Click **Next**.

d. **Authenticator App** will prompt you to Approve or Deny the sign-in attempt. Click **Approve**.

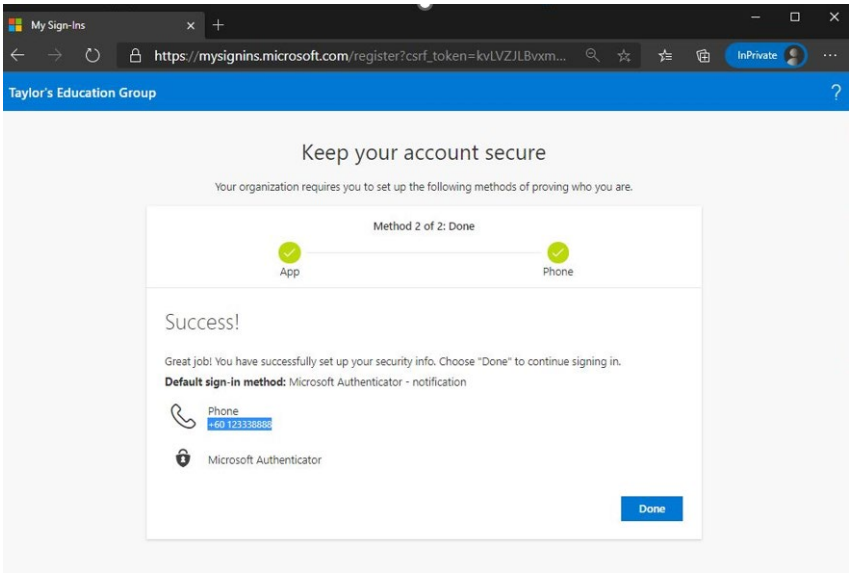


e. You should see a confirmation on your phone registration. Click **Next**.




f. To complete the process, click on **Done** to complete the sign-up process.

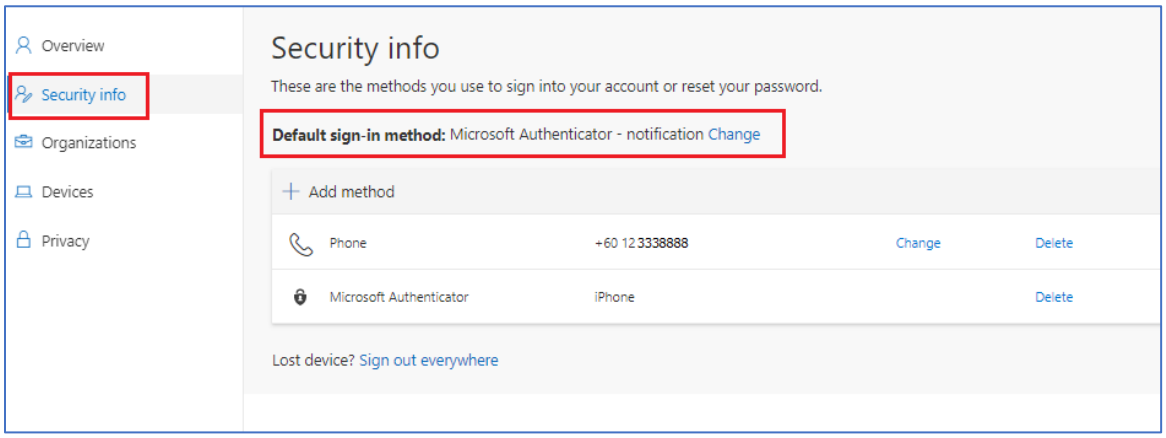


## 5. Optional: Set Phone (SMS) as Default Sign-In Method

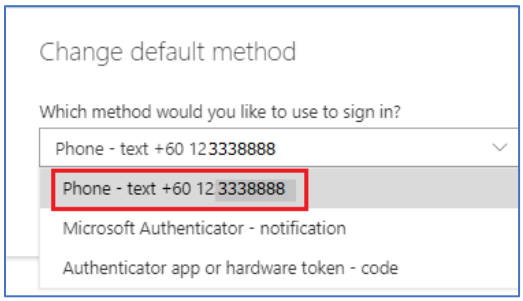
We recommend setting your Phone (SMS) as the default sign-in method for your MFA initially.

a. Go to your MyAccount Portal (https://myaccount.microsoft.com).

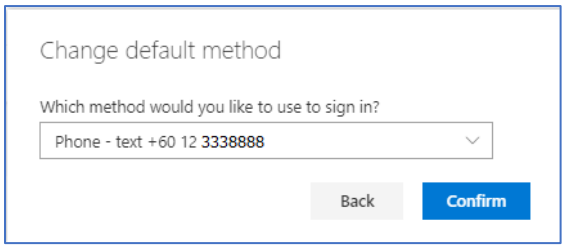
b. Select **Security info** from the left menu and select "**Change**" next to "**Default sign-in method**".




c. When prompted "***Which method would you like to use to sign in?"***, select **Phone.**

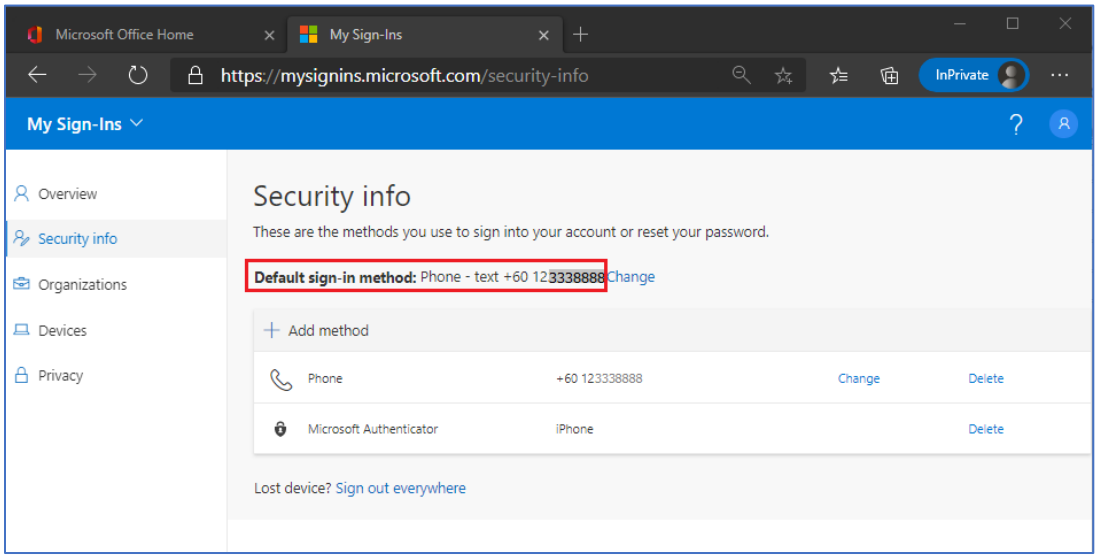



d. Then click "**Confirm**".




e. A message will be shown to confirm your changes.


f. You should see the **Default sign-in method: Phone** shown.



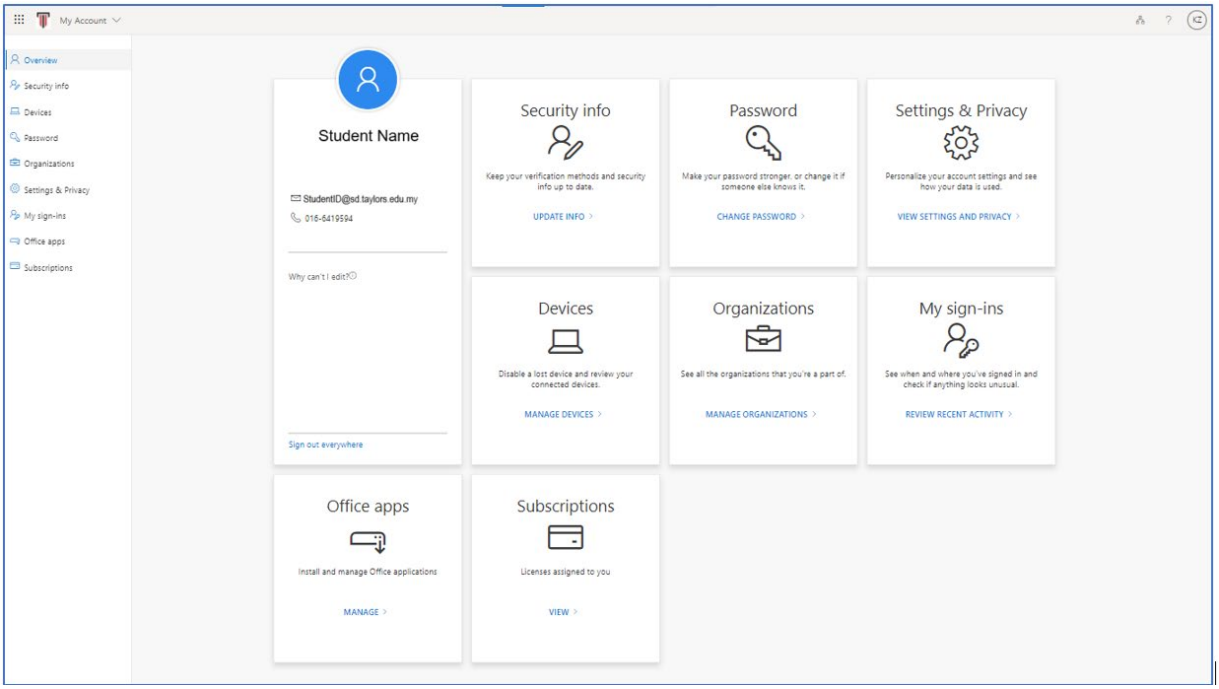

## 6. Re-Launch Office Apps

a) Restart your Computer to ensure MS Outlook, MS Teams and OneDrive are working fine.

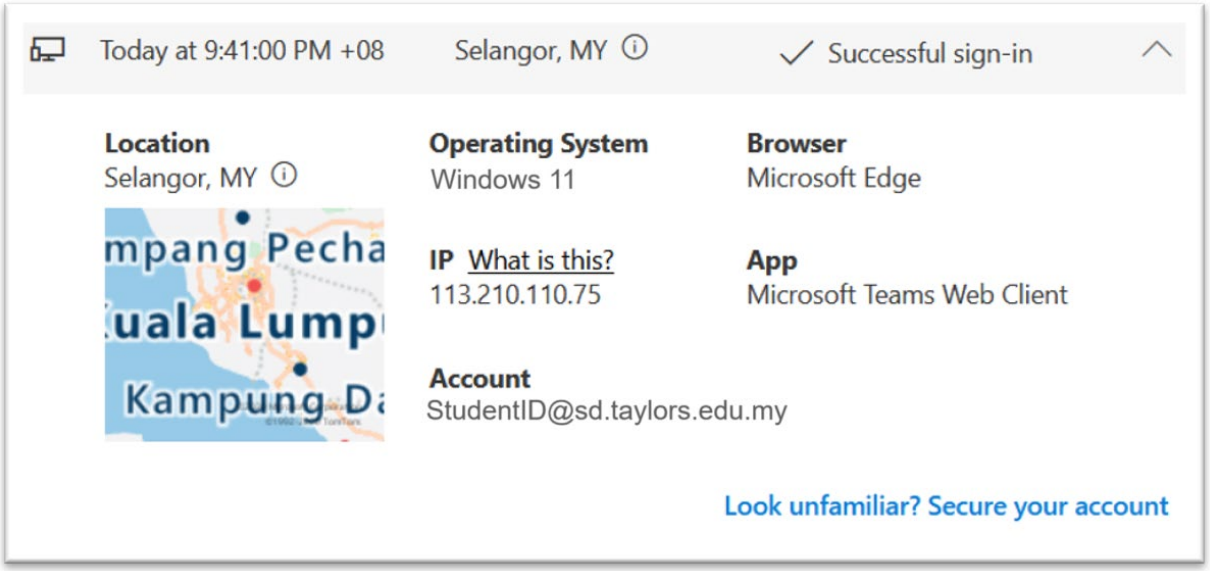
b) Upon successful completion of the above steps, you may proceed to configure email access on your Phone.

# MyAccount Portal

1. Use your MyAccount portal (myaccount.microsoft.com) to manage your security information, your devices, your licenses and change your password.




2. You can also monitor your sign-ins, report suspicious activities and secure your account.



In summary, you can use your MyAccount portal for all your online credential security needs:

- to change default authentication method
- update security info such as phone number
- update password
- manage your devices
- manage guest accounts
- view recent sign-in locations
- download office installer
- view license subscription entitlement

**--- The End ---**