Multi Factor Authentication

Here is a nice concise video outlining the steps that you'll likely benefit from watching first: https://channel9.msdn.com/posts/Multi-Factor-Account-Setup but I've run through the steps again below with screenshots. 😊

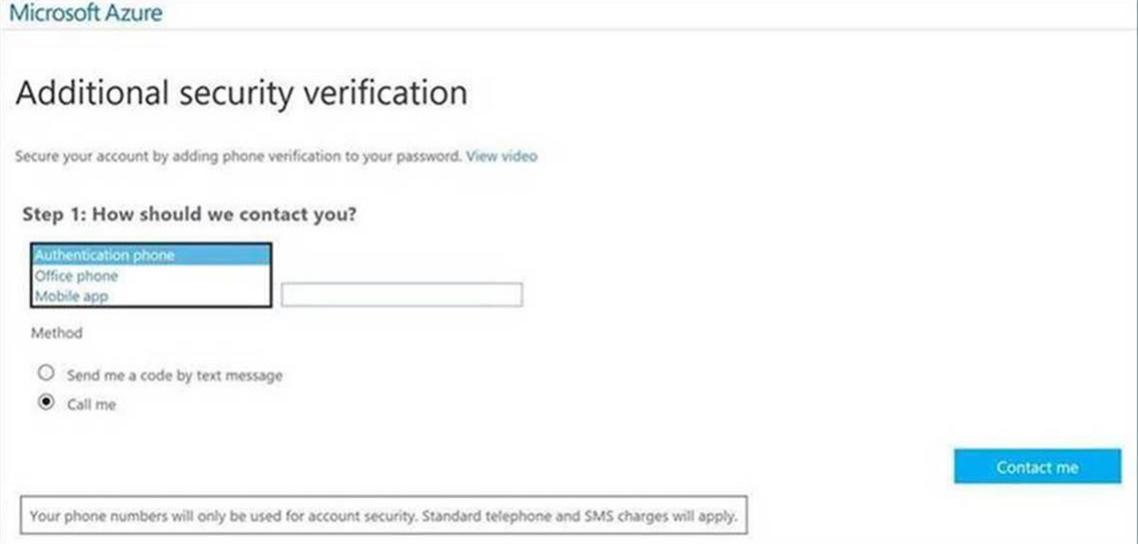**Setting up your authentication methods:**

Click: https://portal.office.com to login to Office 365

Once you login with your normal Office 365 password (your email password), you'll see a security message. Click the button "Set it up now"

You'll need to choose your preferred second method of authentication. (How Microsoft will confirm each log in is actually you)

You can choose any of the 3 methods below to authenticate on going, in fact we recommend setting up multiple methods in case one day you're out of mobile reception or cant log in to emails or phone battery is dead.

Option 1 - Authentication Phone
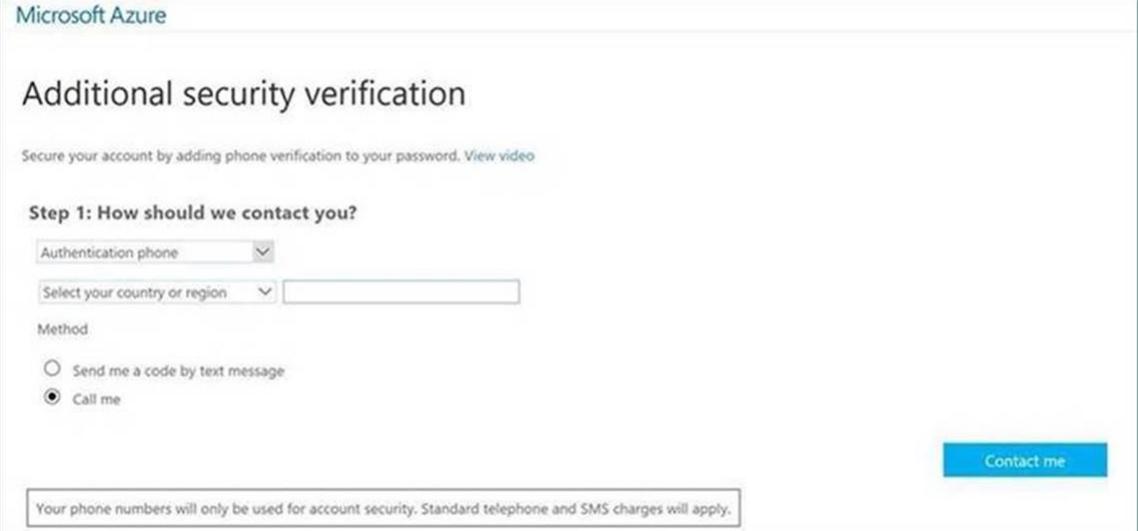
This option is the most sommon and will text you a 6 digit code to the phone number you put it. It doesn't matter if you enter the 0 with your mobile, the +61 for Australia is automatically added. So entering 0439XXX550 will work just as well as entering 439XXX550

Option 2 - Office Phone
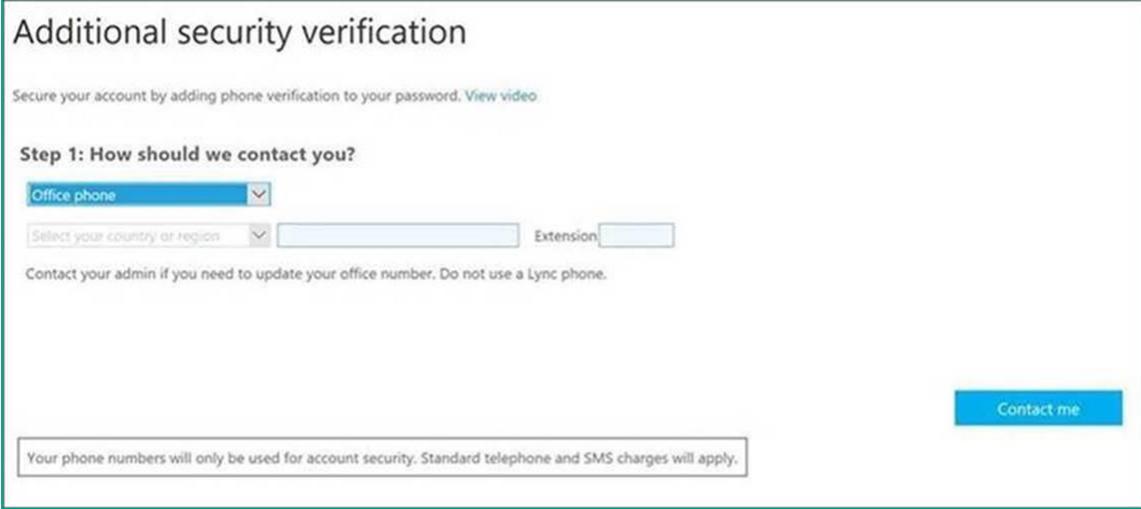
This option you can enter your direct landline number if you don't want to have it connected to your mobile phone. This could be set up as a second method should you ever leave your mobile at home, but is an uncommon choice for the main method of secondary authentication.

Option 3 – Microsoft security Mobile App or Via Google Authenticator
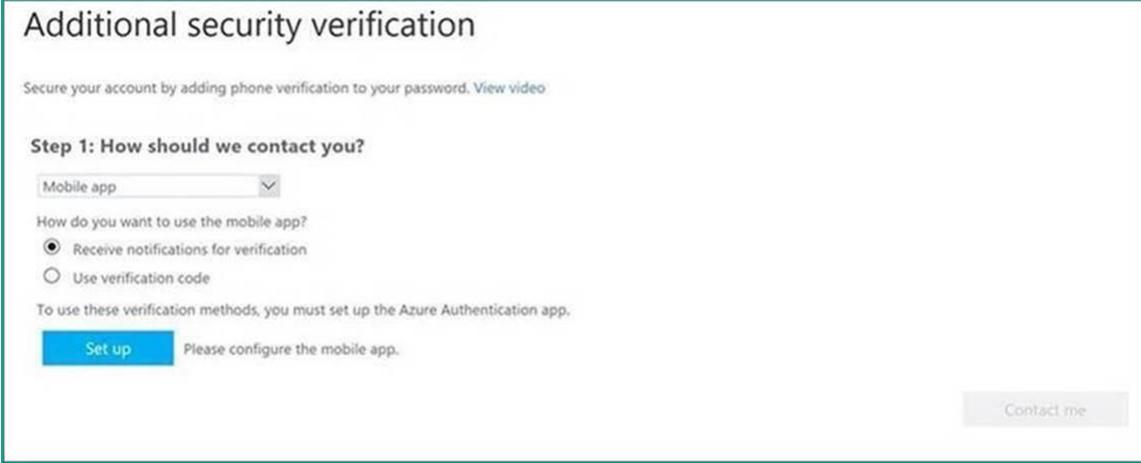
This method uses a mobile app with codes instead of texting them to you. It's a common choice for setting up your Multi-Factor Authentication, and there aren't really any real pros or cons over using the app instead of the texts, other than you don't have to wait for a text as the codes in the app are always present and reset every 30 seconds. When logging in to Office 365, the app can also popup a notification for you to approve or reject the login attempt, instead of having to type the code in.

On your phone, Search in your phone's App Store for "Microsoft Authenticator" (should be ios, android and Windows versions available. If you have a phone other than this, you'll have to use a different verification method)
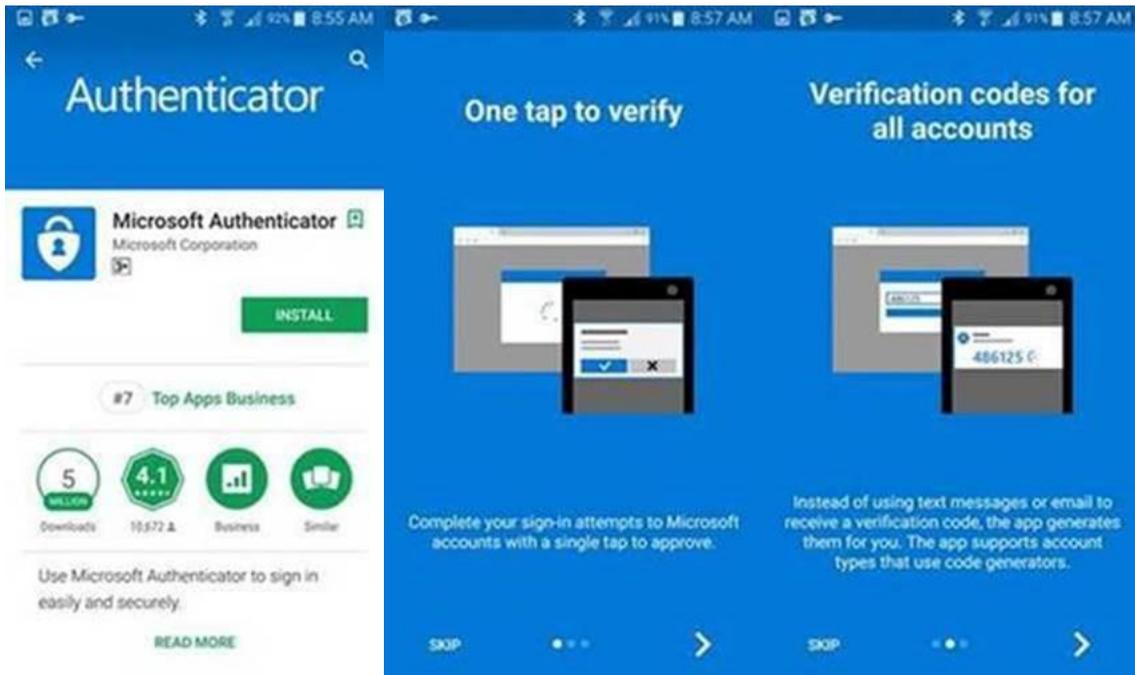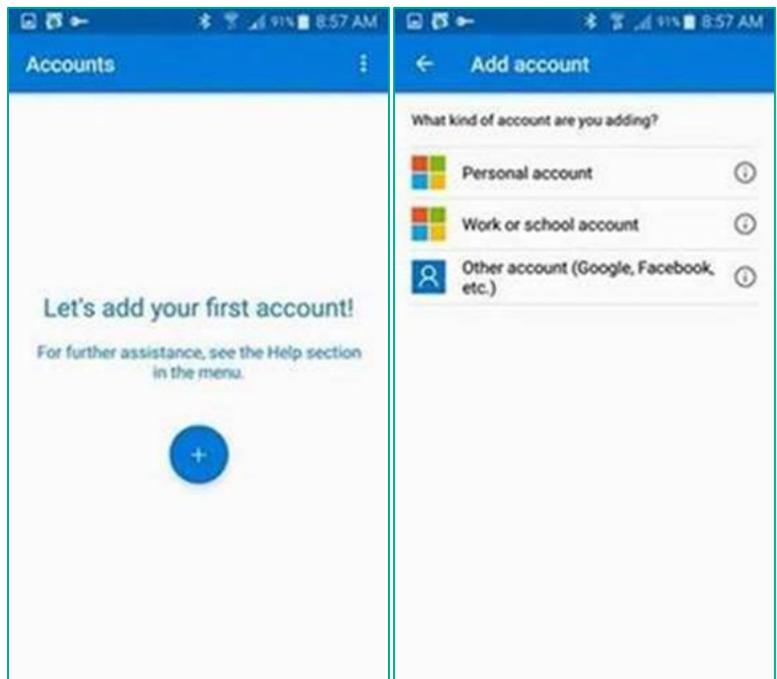

Data Privacy > Ok

+ new account > Work or School Account

Allow it access to your camera, and scan the QR code on your configuration screen
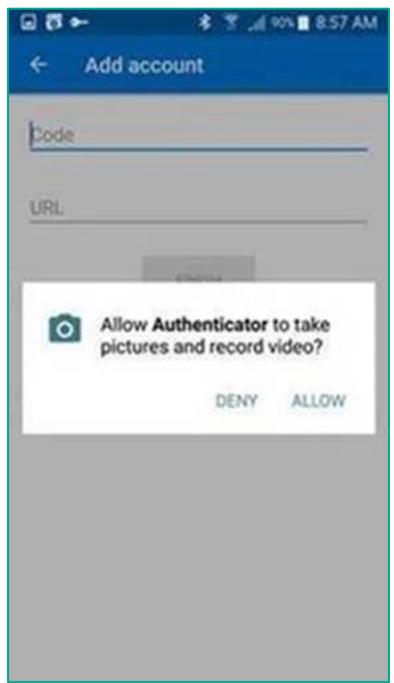
Just line the camera up with the pixelated square QR code, hold it still and tap camera to focus. It will auto register once it finds it.

If you think its lined up and its still not registering, try changing angle of your camera, go slightly closer or further away, tap to focus.

Once QR code is successful, it provides a verification code to enter on the computer.
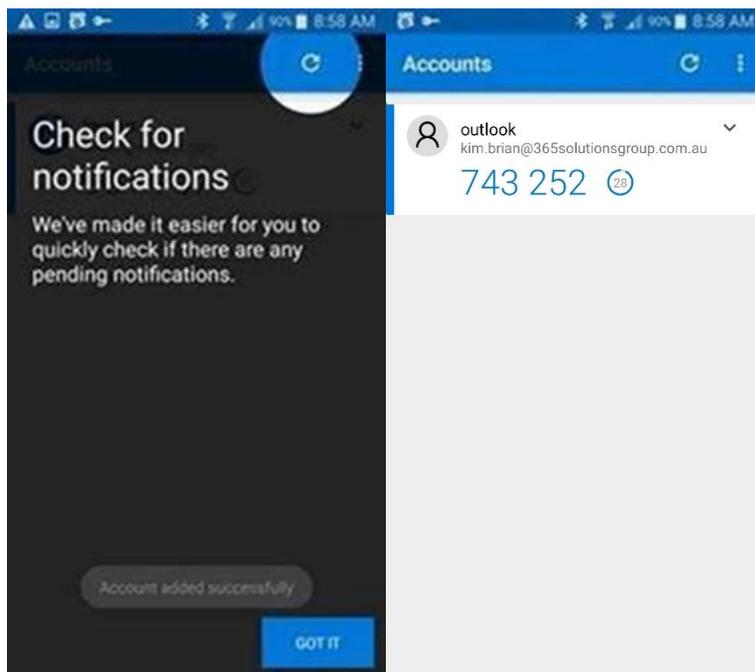
Or if you already have google authenticator app you can click to configure app without notifications link

This will provide a new QR code that will work with any authentication app including google

Once you've chosen an option and confirmed your second method of authentication, you'll be ready to click **Verify.**
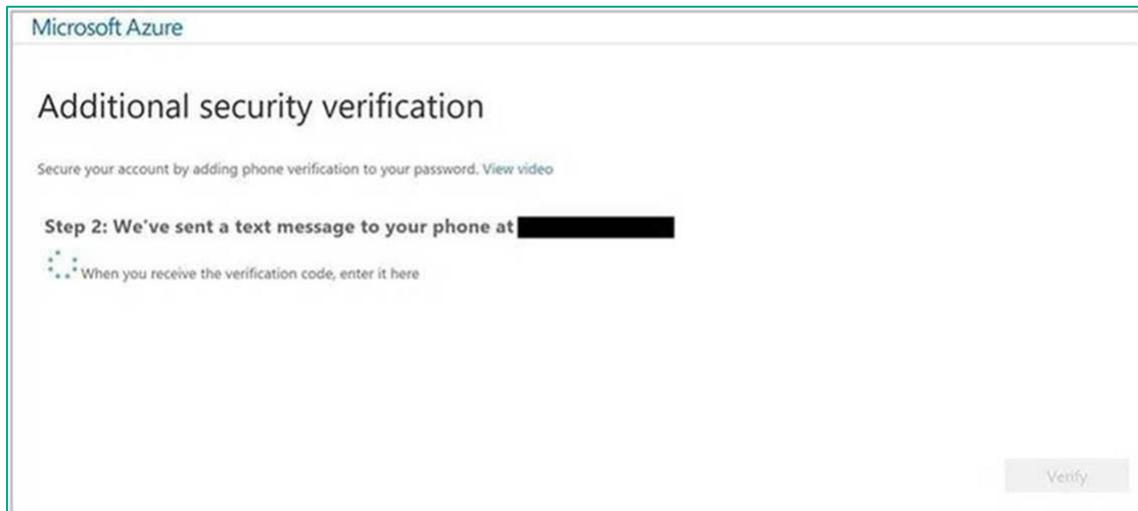
Congrats. You're now authenticated as a user in the browser.

You'll likely then see the page below with an app password. If you're using an up-to-date Windows device, you can just click **Done**.
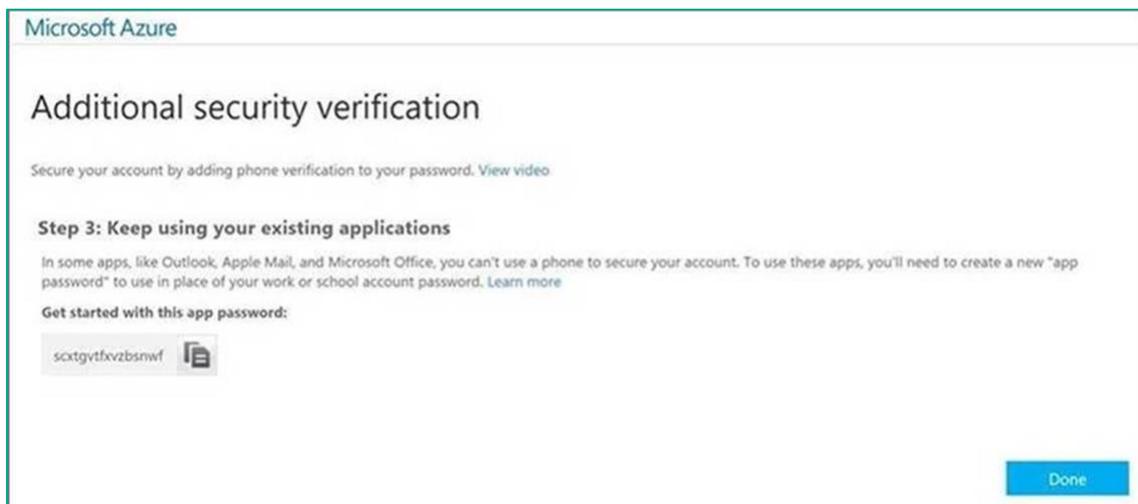
NOTE: The 2019 update to Office 365 means that Outlook and your other applications, including Outlook on your mobile are all configured to work seamlessly with Multi-Factor Authentication. However, if you're using an Apple Mac, an old version of Office outlook, or other applications like other mail applications, you may experience that your password doesn't work when logging in to your work emails, in which case you'll need to set up an App Password

2. Setting up your App Passwords

What is an app password? You use this in place of your original password with non-browser apps (Skype for Business [previously called Lync], Outlook and Office Applications). This is because when you have two-step verification enabled, you're telling Microsoft not to let anyone sign in with your password. The solution to always have access to your applications without a browser login, is to create a more secure *app password* that you don't use day-to-day, but only for those device apps. You use the app password so that apps can bypass multi-factor authentication and continue to work, even when resetting your passwords or completing the 2 step verification in the browser.

How are App Password's more secure?
1. They're longer and randomized so less likely to be guessed or hacked
2. It's a unique direct connection from one application on one device to the Office 365 tenant.
3. They're one use only. So once you've used an App Password to authenticate the version of Outlook on your laptop. It can never be used ever again by any other user or application. These means you need a different App Password for each of your apps. But even if a hacker gets a copy of an app password, it's no use to them because it's already been used by you.

How to use it?

1. You'll see the screen below, copy the long string of letters in the box. This is your first App Password. You can write it down, or Ctrl + C when it's selected to copy the password. (Remember once you click ok/close you can NEVER SEE THAT APP PASSWORD AGAIN so make sure you enter it straight away.
2. Close Outlook and open it again.
3. When prompted for your password enter the new app password (write it in or Crtl + V to paste) INSTEAD of your normal password.
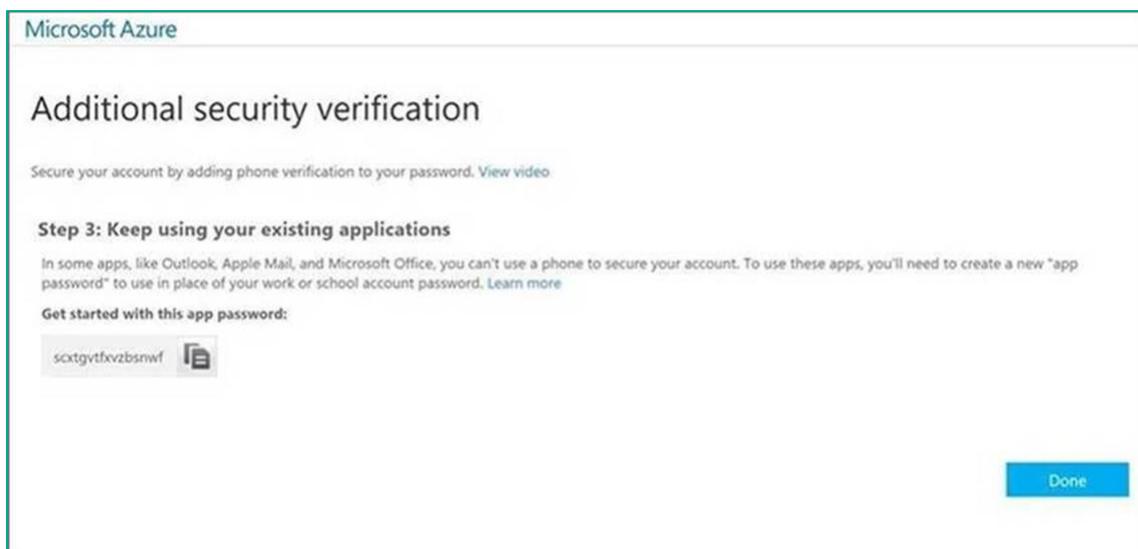
4. You'll need to enter a new App Password for each app that asks, for each device you use that app on.
   So if you use Skype for Business on you laptop, PC and Phone, and Outlook on your Laptop, PC and phone, you'll need 6 app passwords.
5. So you'll need to go to the app password page, generate a new one for each app. Eg one called "Skype for Business PC", one called "My phone emails". Name doesn't really matter much other than your own reference.
6. When you open Skype for Business, you'll need to forget existing credentials, put in your email address, and a new App Password INSTEAD of your normal password.

Any time you need to put in your password for Office 365, it will either be in an internet browser (like accessing SharePoint) and you'll be asked to verify using the method you chose above (enter app code) or it will be by an non-browser based app like Outlook or Skype that are installed on your machine, which is when you'll need to enter an *App Password* instead of your normal password.
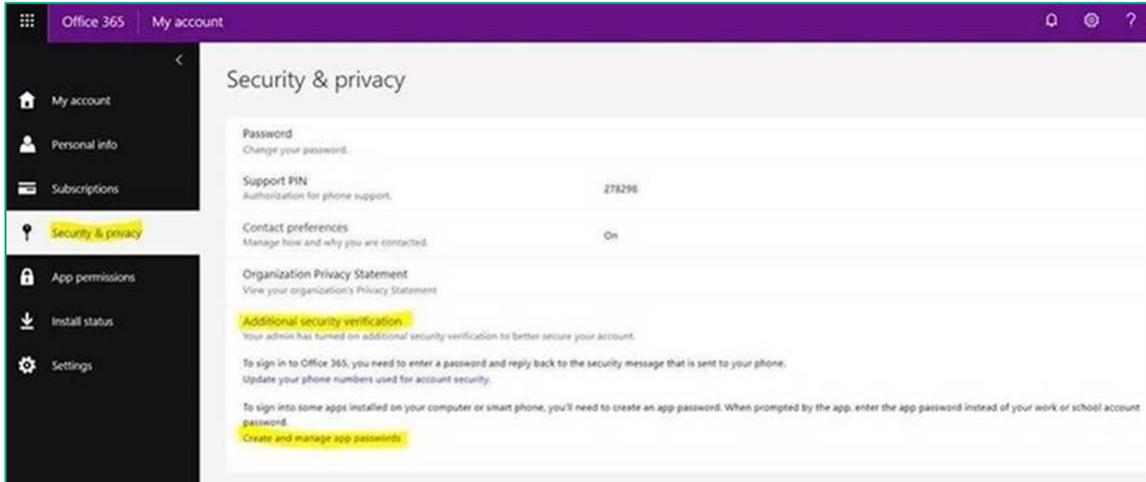
To generate more App Passwords in the future:

1. Go to https://portal.office.com and login (with 2 verification methods)
2. Click your user icon in the top right corner
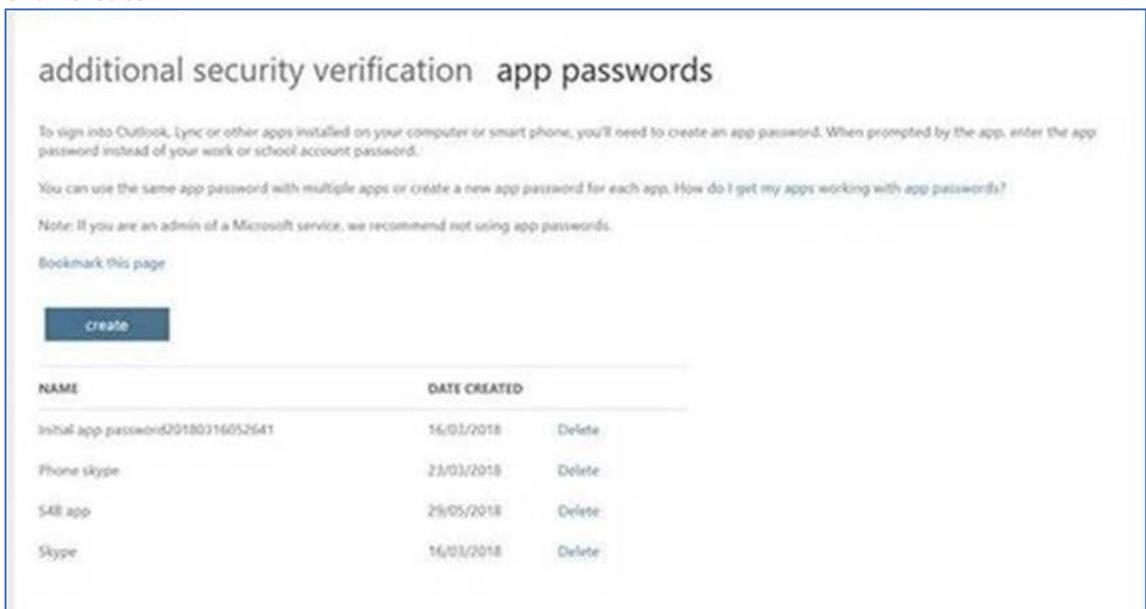3. Click **My Account**
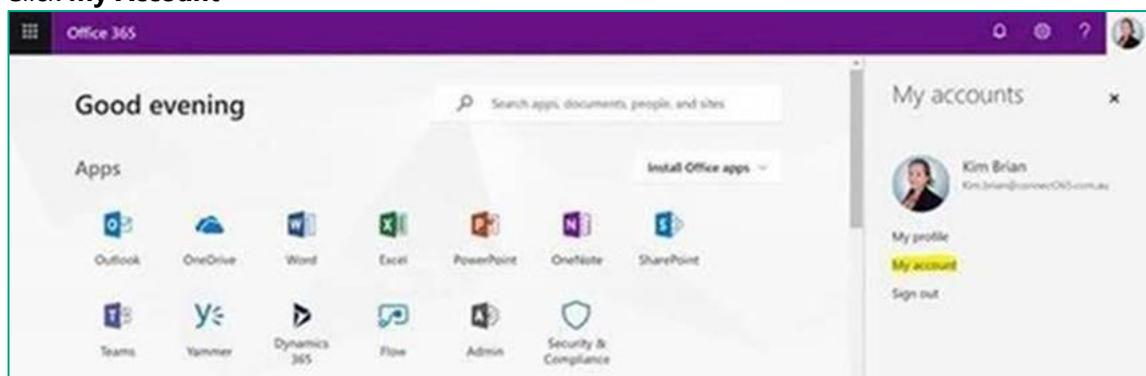
4. Select **Security & Privacy**
5. Click on **Additional Security Verification** at the bottom to expand the section
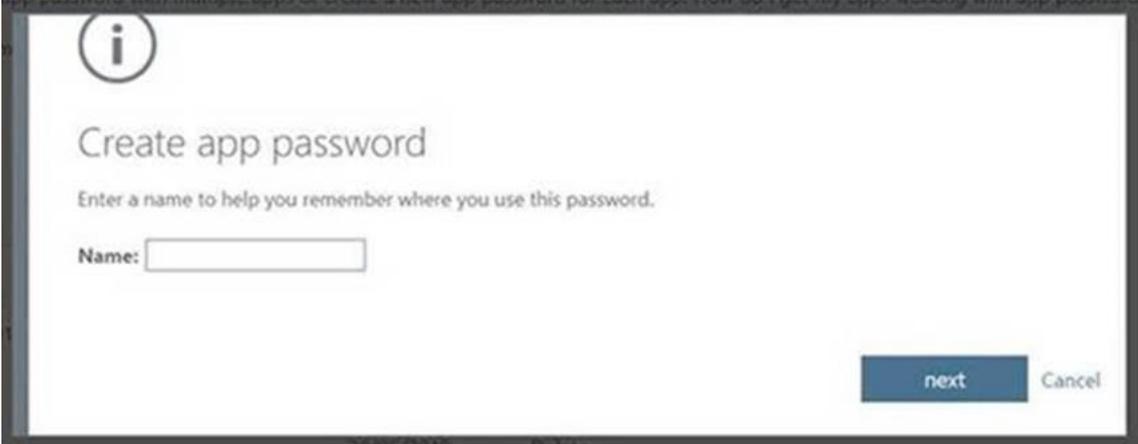
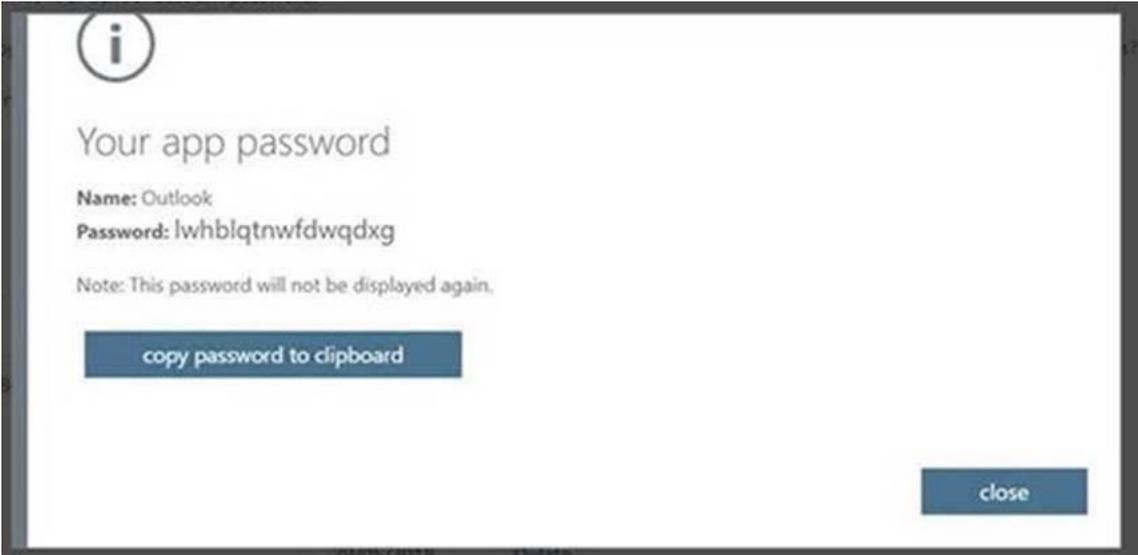6. Click on **Create and manage app passwords**

7. Click **Create**

8. Give your app password a name (this doesn't really matter and is for your reference only. Example "Skype for Business Laptop September 2019" and click **Next**

9. It will generate a new *App Password* to use in your applications. Copy and enter it as instructed above

Remember once you've used an *App Password* to sign in to your application (Skype/Outlook), you wont need to worry about it again. If you need to sign it to that same app again in the future, create a new *App Password* and delete the old one for that application.

If you need to change your phone number you receive verification texts to or other information. Follow the instructions on this [link](#).

If you require any assistance navigating these steps, you may be able to assist each other internally, otherwise you can **reach out to me for help with this MFA matter via** support@365sg.com.au *or by calling us on 1300 228 744.*
.