
# Setting up Multi-Factor Authentication

A Cyber Security Guide

Brock University

# Multi-Factor Authentication

## Overview

**Multi-Factor Authentication** (**MFA**) is a security system that requires you to provide more than one form of identification at the time of login to ensure you are who you claim to be. It combines at least two forms of authentication: something you know (e.g., a password) and something you have (e.g., a cell phone or a code generator).

This guide explains the different authentication options available to you, and steps you through the entire process of getting Multi-Factor Authentication set up and enabled on your account.

There are 2 steps involved in getting set up with MFA on your account:

1. Choose which device you will use to verify your identity
2. Enable Multi-Factor Authentication on your Brock account

**NOTE:** You will need access to a computer and have your mobile device on hand to complete MFA setup.

## Choose which device you will use to verify your identity

In order to log in and access your Brock account, you are required to input your password and then verify your identity using either your mobile device or a One-Time Verification (OTV) Code Generator device.

It is good practice to set up more than one way to verify your identity, as there may be times certain authentication methods will not be available to you (for example, some methods do not work overseas). Enabling multiple authentication methods will ensure you can always access your account.

### Using your mobile device

If you wish to use your mobile device to verify your identity when you log in, you have four options of how to do so. You can:

- respond to a notification from the **Microsoft Authenticator** app installed on your device (recommended)
- enter an authentication code generated by the **Microsoft Authenticator** app installed on your device
- receive an SMS text message with a 6-digit authentication code that you will enter during login
- receive a phone call and follow the prompts to verify your identity

If you decide to receive either SMS text messages or phone calls, you can skip ahead to **Enabling Multi-Factor Authentication on your Brock account** (pg.4). However, if you decide to use the **Microsoft Authenticator** app, you need to install the app on your mobile device first (see installation instructions on next page).

## Installing the Microsoft Authenticator app

If you wish to use an app on your mobile device to generate authentication codes, you will need to install the **Microsoft Authenticator** app on your device (free on Android and iOS).

To install the app on Android:

1. On your Android device, open the **Play Store** app
2. Search for **Microsoft Authenticator**
3. Select **Microsoft Authenticator** from the search results and tap **Install**
4. If asked to authorize Microsoft Authenticator to access information on your device, tap **Accept**. You'll be returned to the app screen. Press the **back button** to return to your home screen.
5. The app should now be on your home screen. Tap the icon to run the app.

To install the app on iOS:

1. On your iOS device, open the **App Store**
2. Search for **Microsoft Authenticator**
3. Select **Microsoft Authenticator** from the search results and tap **Get**
4. The app should now be on your home screen. Tap the icon to run the app.

Once you have installed the app, go on to **Enabling Multi-Factor Authentication on your Brock account**.

## Using a One-Time Verification (OTV) Code Generator


A **One-Time Verification** (**OTV**) **Code Generator** is a small device with a built-in screen that generates and displays authentication codes for MFA logins.

One-Time Verification Code Generators are activated and linked to your Brock account by an admin in ITS. If you wish to use an OTV Code Generator, contact the ITS Help Desk for assistance.

Once you receive an OTV Code Generator no further steps are necessary for you to set up and enable Multi-Factor Authentication on your account (configuration is completed by ITS).

**NOTE:** You cannot use an OTV Code Generator for multi-factor authentication when trying to establish a Remote Desktop connection. You must use one of the other authentication methods presented in this guide when using Remote Desktop.

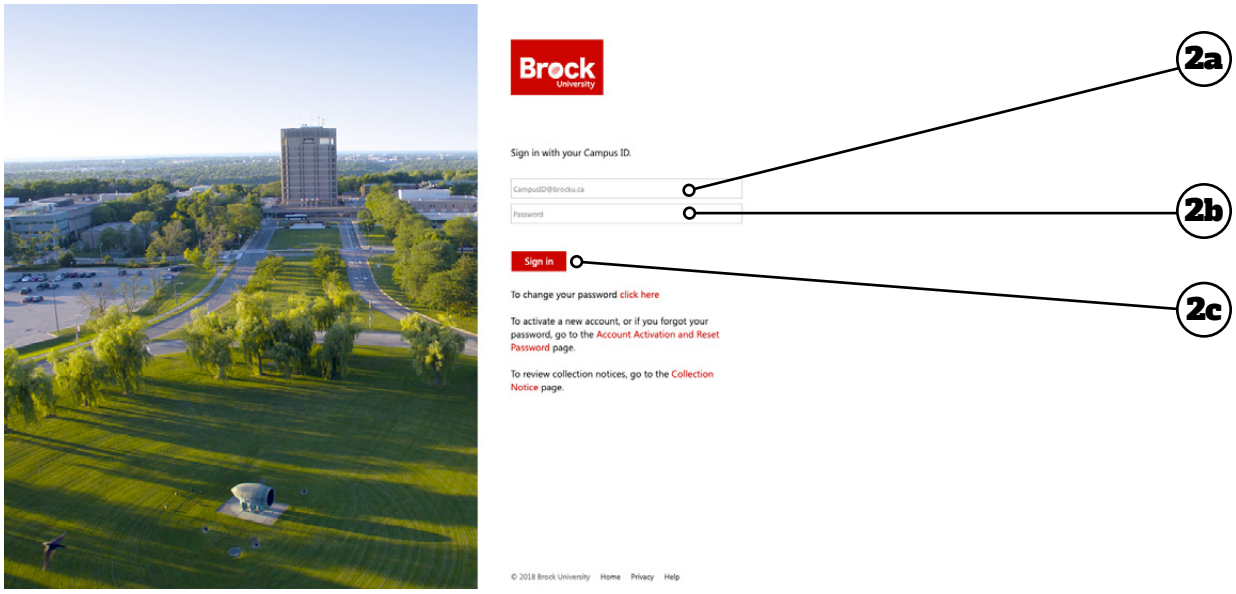
# Enabling Multi-Factor Authentication on your Brock account

When you log into your Brock account, you may receive a dialogue box indicating that more information is required to keep your account secure. If you do, click **Next** and then follow the steps presented in this guide (starting with step 3) to set up MFA on your account.

**A.** If you see this dialogue box when you log into your Brock account, click **Next** and then skip to step 3. Otherwise, see step 1 below.


**1.** If you do not see the dialogue box shown above when you log into your Brock account, you can manually enable Multi-Factor Authentication on your account. Go to [aka.ms/mfasetup](aka.ms/mfasetup) and select your account from the list.

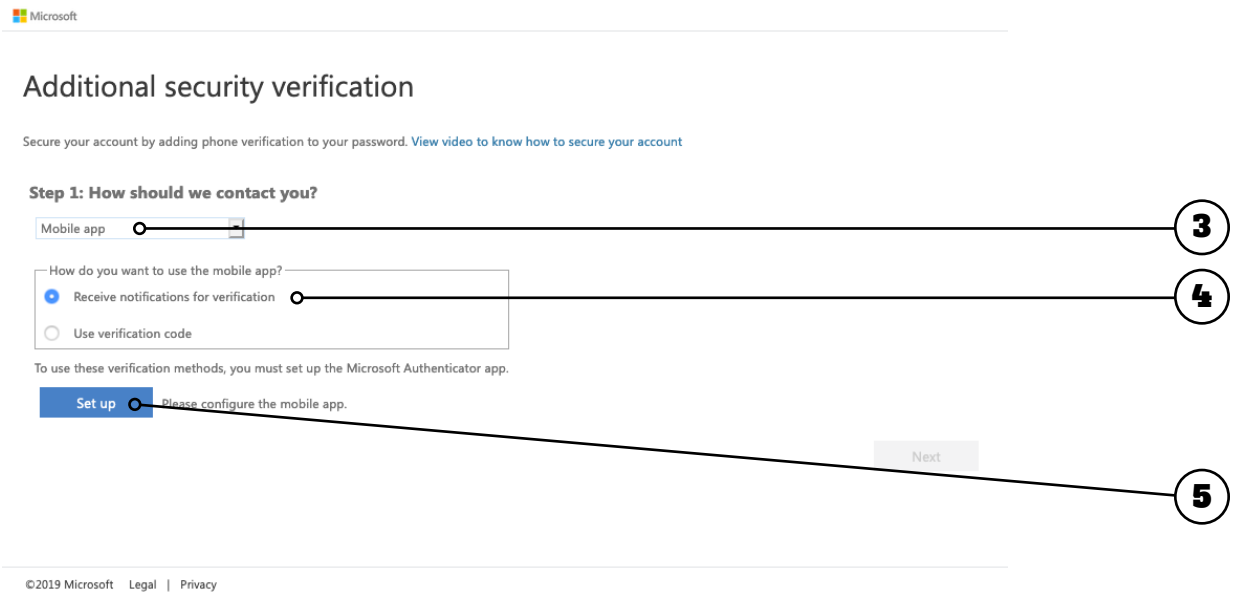

**2.** Enter your **Campus ID** (**2a**) and **password** (**2b**), then click **Sign In** (**2c**).



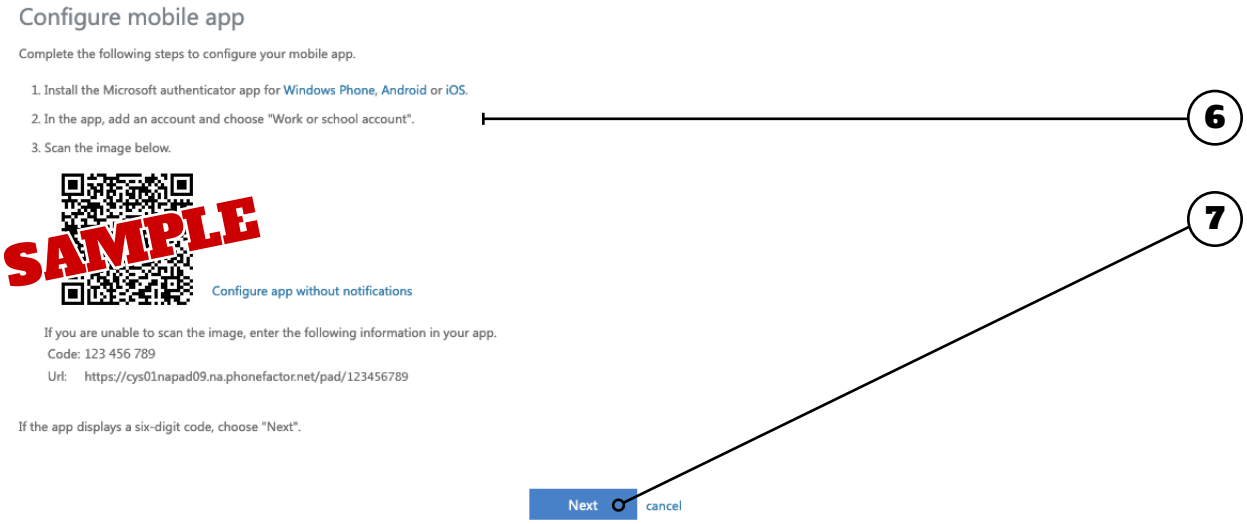
## OPTION 1 - Respond to notifications from the Microsoft Authenticator app (recommended)

If you wish to verify your identity by responding to push noifications from the Microsoft Authenticator app on your mobile device:

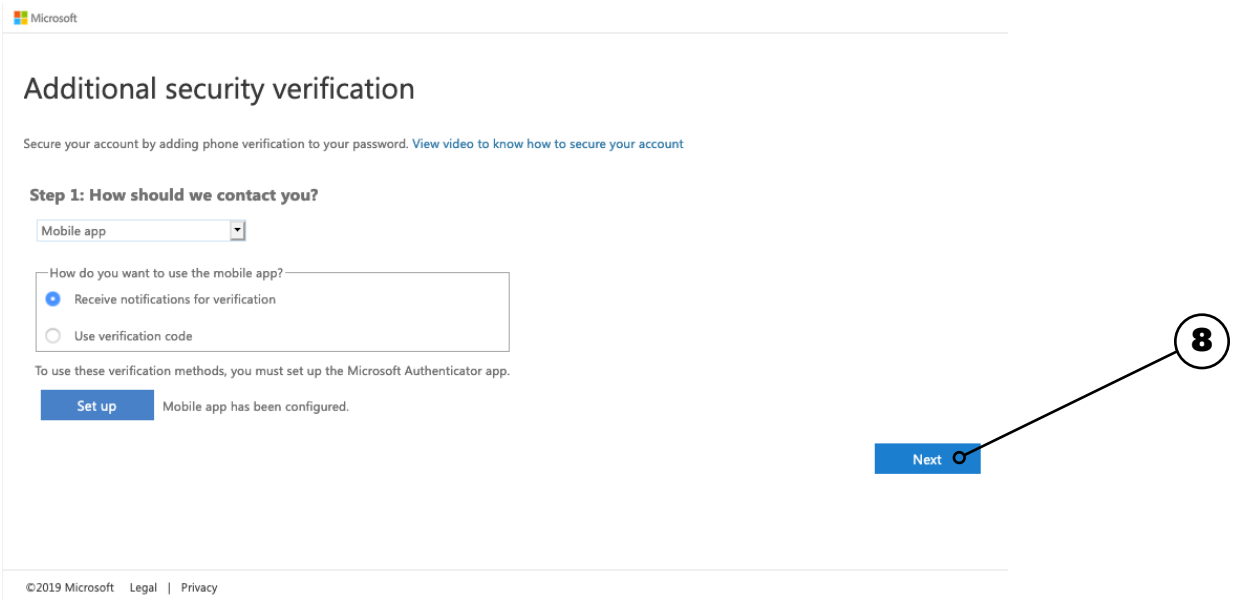
3. Choose **Mobile app** from the dropdown menu.
4. Select **Receive notifications for verification**.
5. Click **Set up** to configure the mobile app.




6. The **Configure mobile app** screen will appear in your browser. Follow the steps shown.
7. Once you have successfully configured the app, click **Next**.

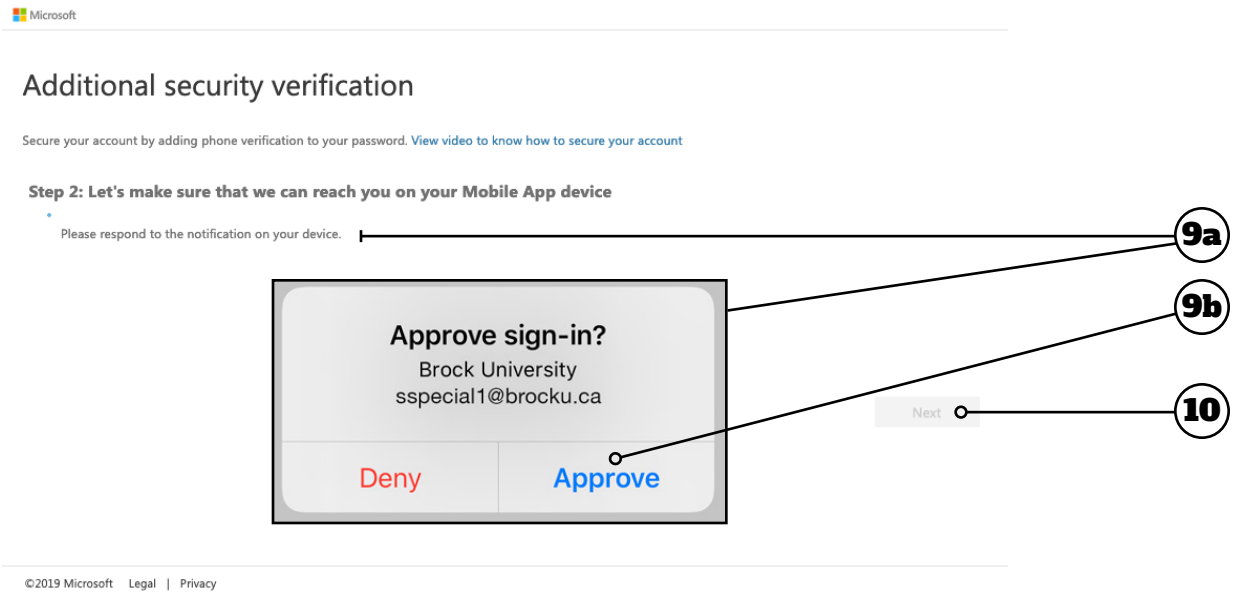


8. You will return to the previous screen, but now you can select the Next button to proceed. Click **Next**.




9. The app will send you a push notification on your mobile device asking you to approve sign-in (**9a**). Click **Approve** (**9b**).

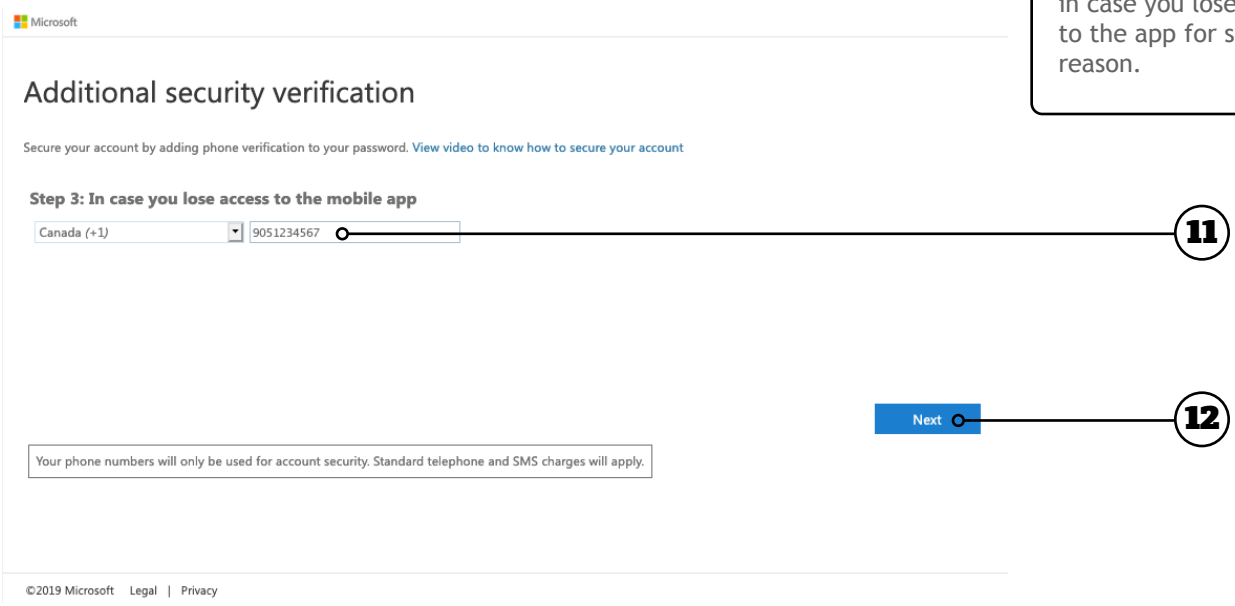
10. Once the system has successfully processed your approval, the Next button will become active. Click **Next**.



**11.** Enter your mobile phone number.

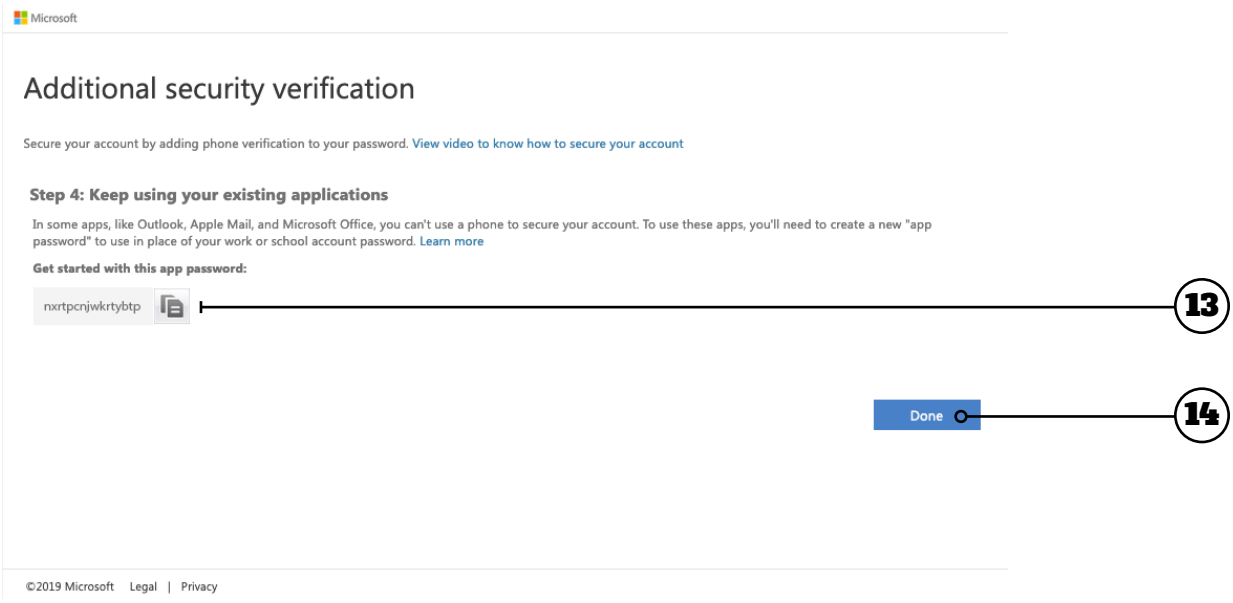
**12.** Click **Next**.

Your phone number is needed as a backup authentication method in case you lose access to the app for some reason.




**13.** Take note of the app password displayed - you will need this when using certain apps like Apple Mail or Office (local install) on your phone and desktop.

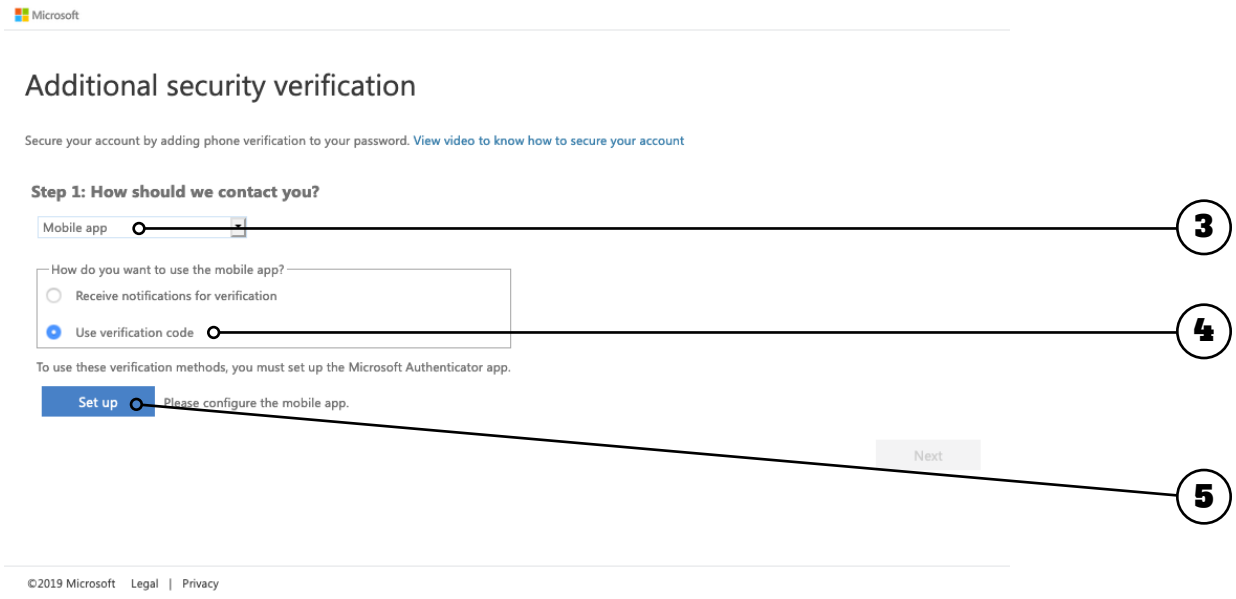
**14.** Click **Done**.



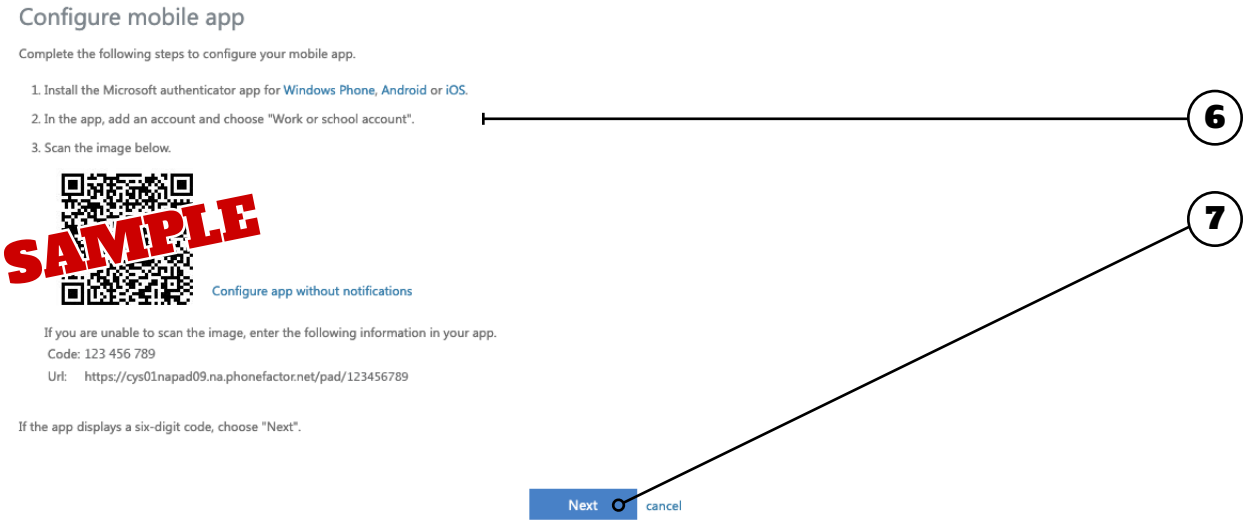
## OPTION 2 - Enter codes generated by the Microsoft Authenticator app

If you wish to verify your identity by entering the codes generated by the authenticator app:

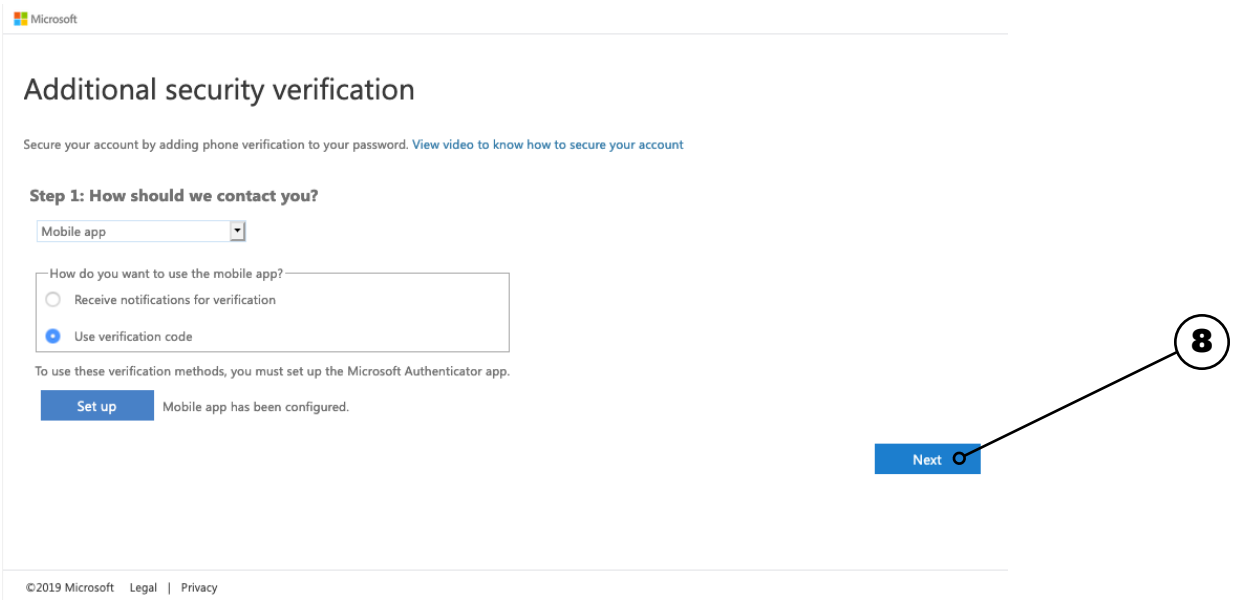
3. On the next screen, choose **Mobile app** from the dropdown menu.
4. Select **Use verification code**.
5. Click **Set up** to configure the mobile app.




6. The **Configure mobile app** screen will appear in your browser. Follow the steps shown.
7. Once you have successfully configured the app, click **Next**.



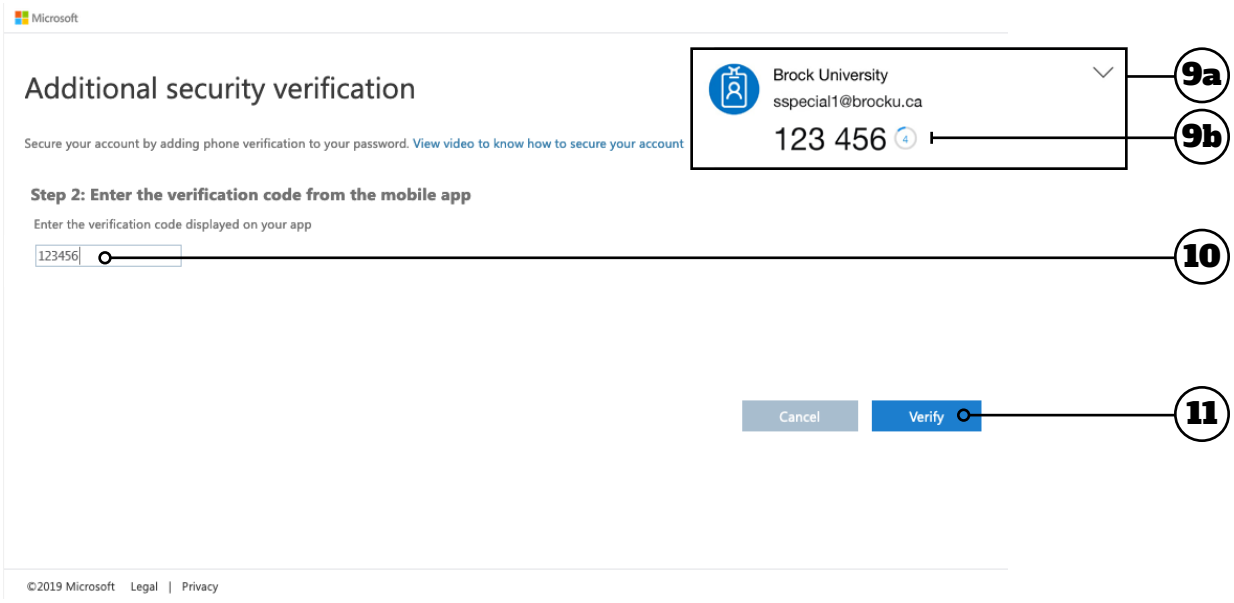
8. You will return to the previous screen, but now you can select the Next button to proceed. Click **Next**.




9. In the app on your mobile device (**9a**), you will see the **current code** for your Brock University sign in (**9b**). Note the timer to the right of the code. A new code is generated every 30 seconds and you must type in the code as it is currently displayed, so a good rule of thumb is that if the timer is almost up, wait for the next code to be displayed before you begin typing it in.

10. Type in the **current code** (without spaces).

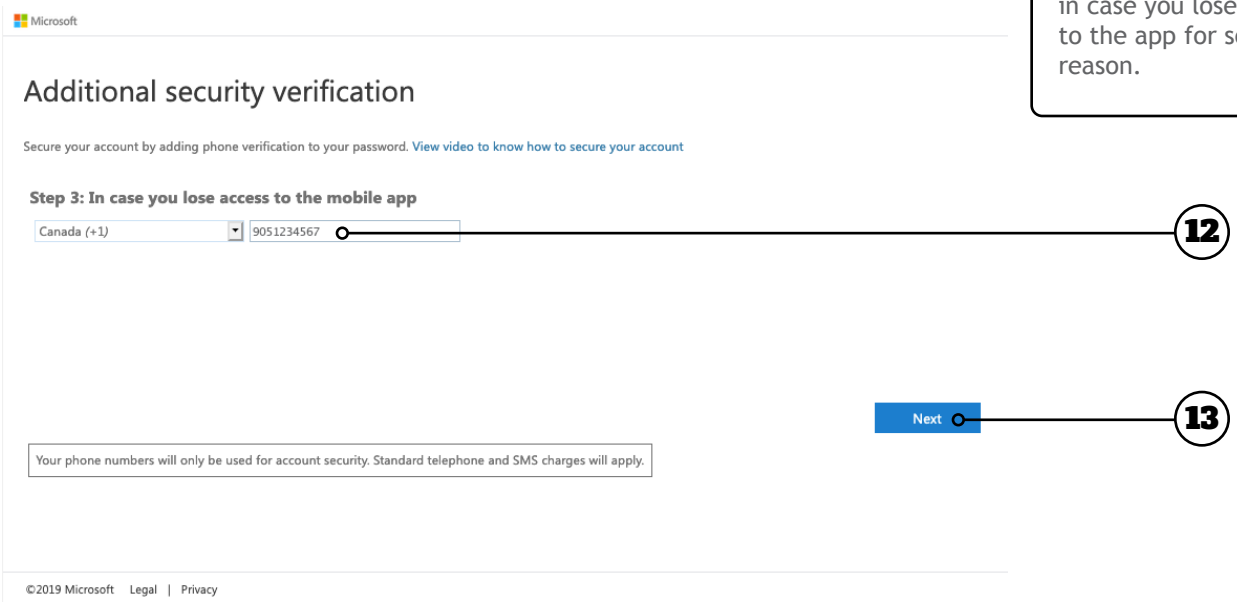
11. Click **Verify**.



**12.** Enter your mobile phone number.

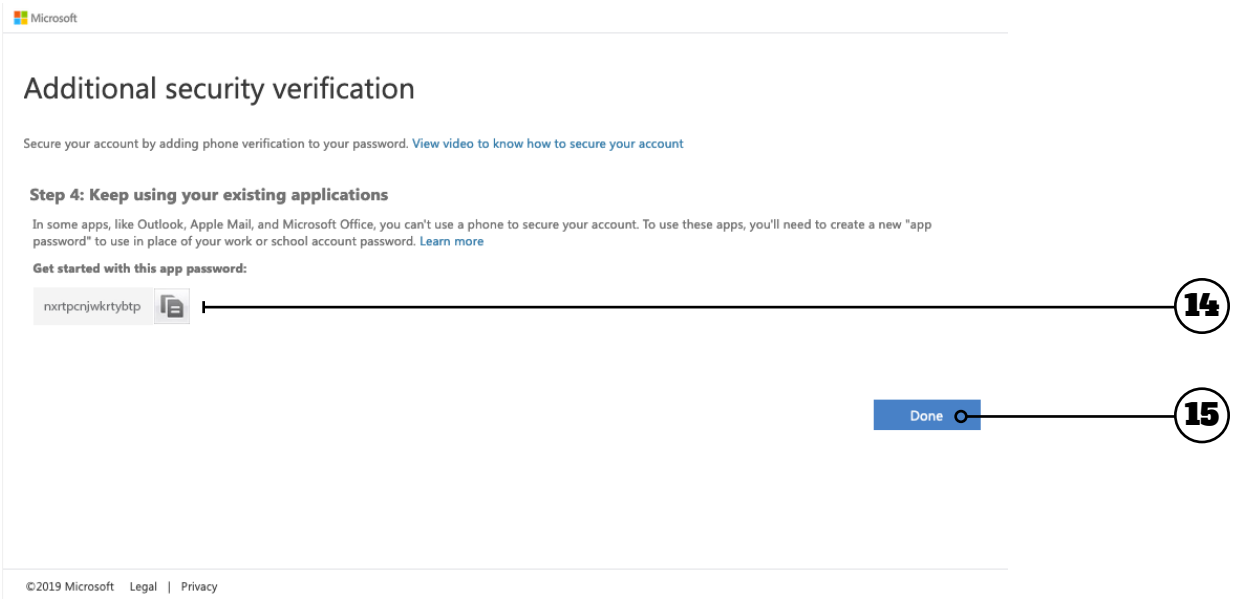
**13.** Click **Next**.

Your phone number is needed as a backup authentication method in case you lose access to the app for some reason.




**14.** Take note of the app password displayed - you will need this when using certain apps like Apple Mail or Office (local install) on your phone and desktop.

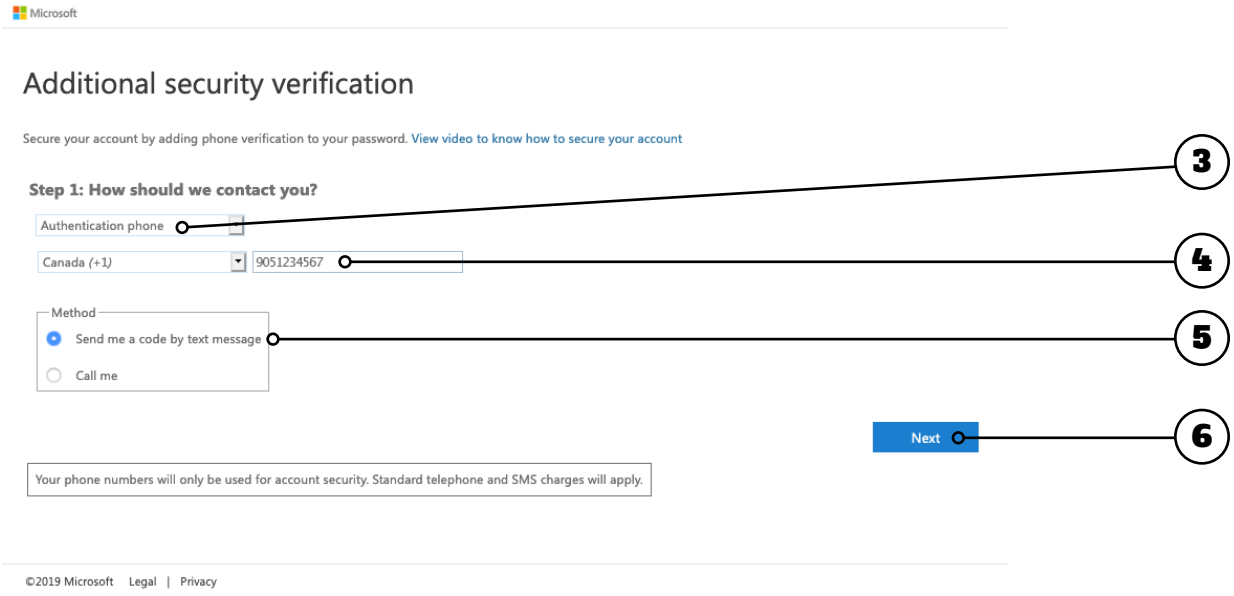
**15.** Click **Done**.



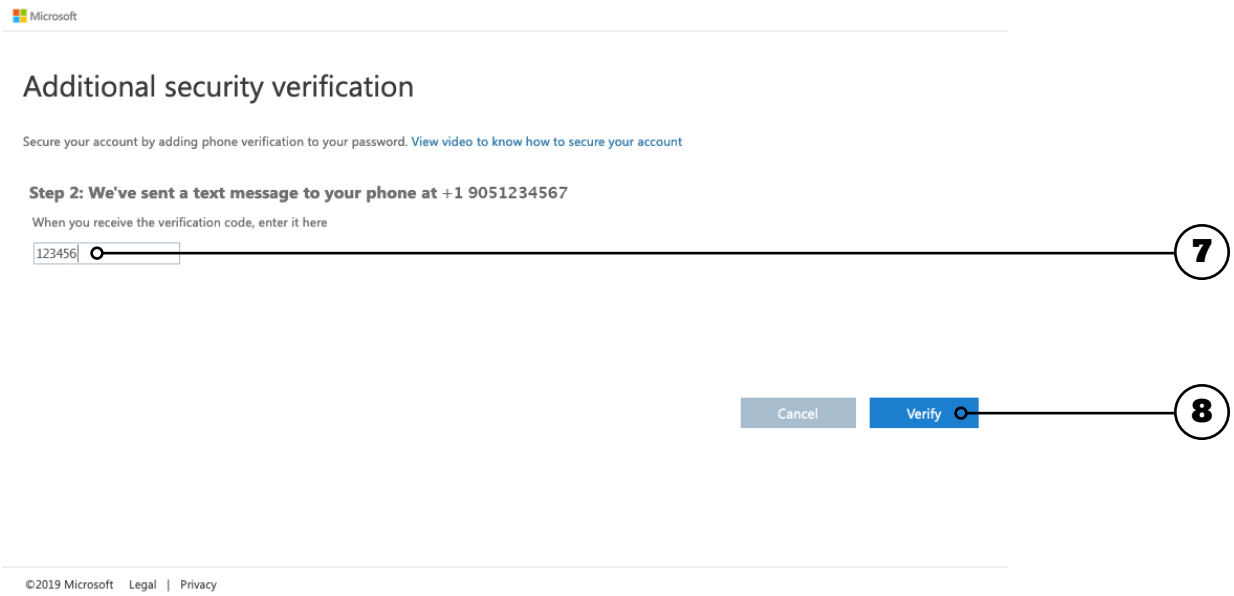
## OPTION 3 - Receive authentication codes via SMS text messaging

If you wish to verify your identity by receiving authentication codes via SMS text messaging:

3. Choose **Authentication phone** from the dropdown menu.
4. Enter your **mobile phone number**.
5. Select **Send me a code by text message**.
6. Click **Next**.

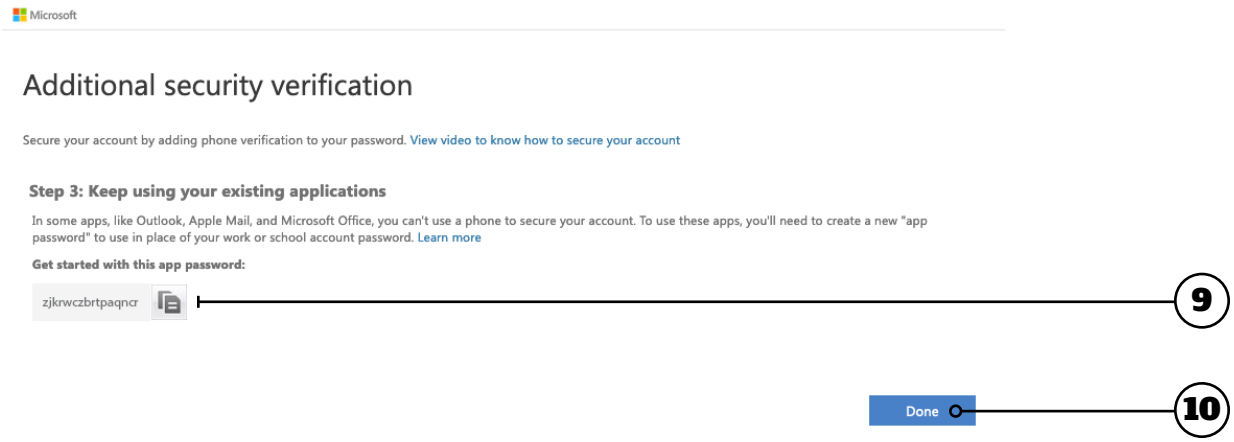



7. You will receive a text message containing a **6-digit code**. Enter that code into the field.
8. Click **Verify**.



9. Take note of the app password displayed - you will need this when using certain apps like Apple Mail or Office (local install) on your phone and desktop.

10. Click **Done**.




## OPTION 4 - Receive phone calls and follow the prompts

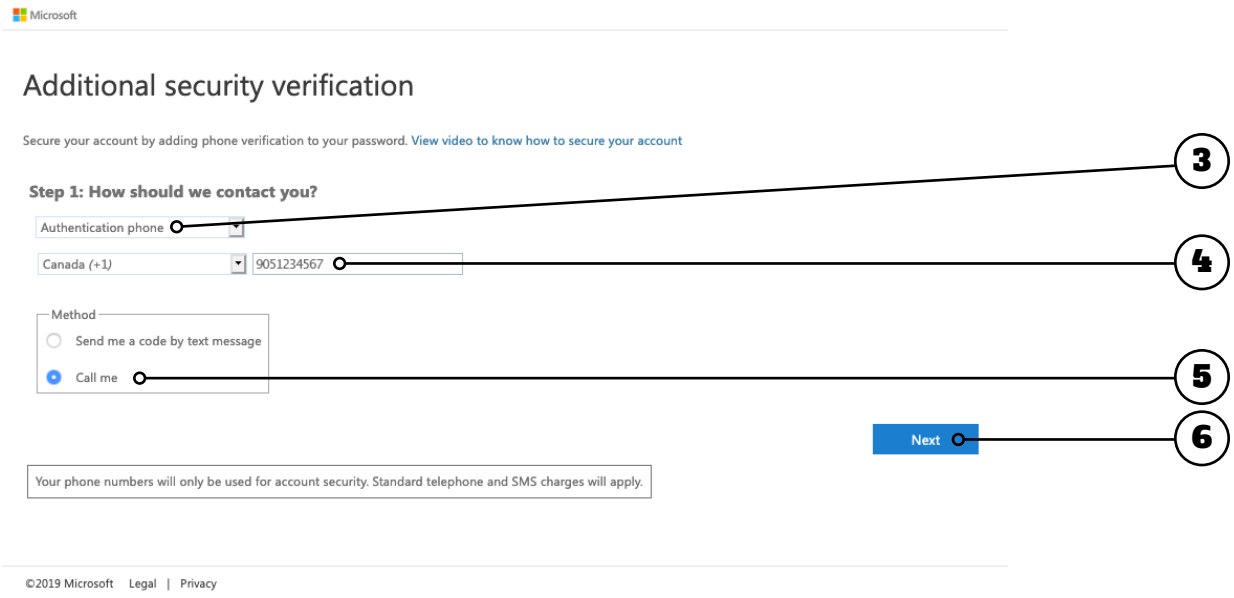
If you wish to verify your identity by receiving phone calls to your mobile device:

3. Choose **Authentication phone** from the dropdown menu.

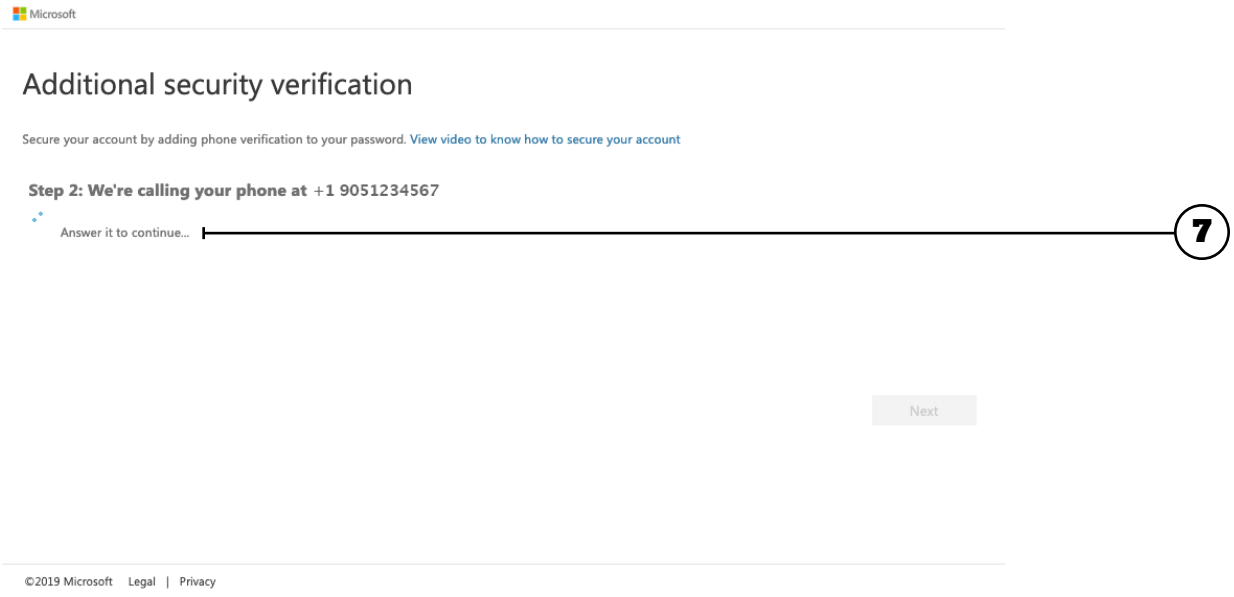
4. Enter your **mobile phone number**.

5. Select **Call me**.

6. Click **Next**.

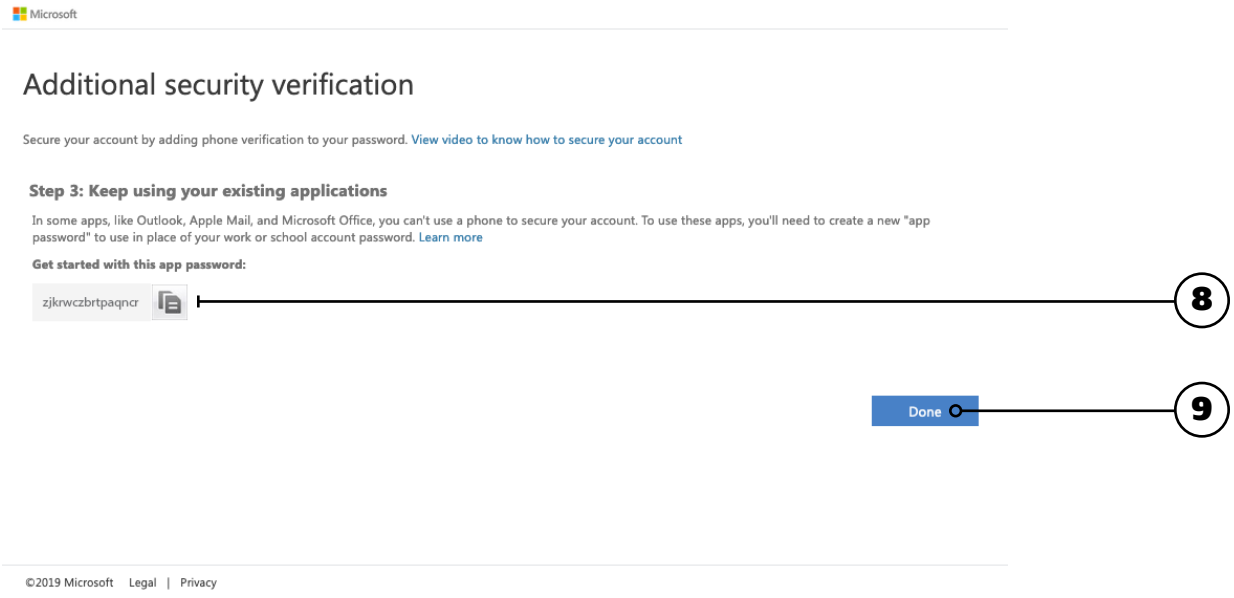


7. You will receive a call on your mobile phone. Answer it and follow the prompts to complete the authentication process. You will automatically proceed to the next screen.




8. Take note of the app password displayed - you will need this when using certain apps like Apple Mail or Office (local install) on your phone and desktop.

9. Click **Done**.



# Additional Resources

## More Information

You can find more information about Multi-Factor Authentication at brocku.ca/information-technology/service-catalogue/security-and-access/multi-factor-authentication/.

## Help Desk Support

If you require technical assistance with Multi-Factor Authentication, please contact the Help Desk at x4357 or ithelp@brocku.ca.

## Other Learning Support

For additional learning support resources, go to brocku.sharepoint.com/information-technology.