

# Multi-Factor Authentication (MFA)

## Quick Reference Guide

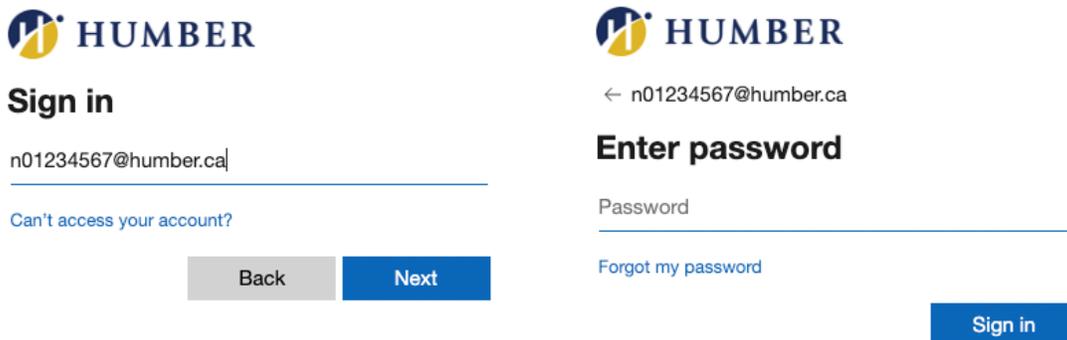
### Preamble

Multi-factor authentication (MFA) is a process where you are challenged for an additional form of identification, such as a code sent to your phone, before being granted access to log onto a Humber webpage. If you only use a password to authenticate, it leaves the possibility of a hack more likely, as some passwords are not very secure, or can be compromised. Using multi-factor authentication increases the security since it will be harder for a hacker to compromise a password AND a mobile device. You will need to have your account added to the MFA group before you will be able to do the set up. Once you have received notification that you have been added to the group, you can follow the steps before.

**Please Note:** You will need your computer AND your mobile device.

### Getting Started

On your computer or laptop, launch a browser and navigate to the website: [myAccount.humber.ca](https://myAccount.humber.ca). You will be directed to the Humber logon page. Enter your username, followed by "@humber.ca" and click **Next**. Enter your password and click **Sign in**.



The screenshot shows two stages of the login process. On the left, the 'Sign in' page features the Humber logo, the text 'Sign in', a text input field containing 'n01234567@humber.ca|', a blue link for 'Can't access your account?', and two buttons: a grey 'Back' button and a blue 'Next' button. On the right, the 'Enter password' page features the Humber logo, the email address 'n01234567@humber.ca', the text 'Enter password', a password input field, a blue link for 'Forgot my password', and a blue 'Sign in' button.

You will then see a page indicating that more information is required. Click **Next**.

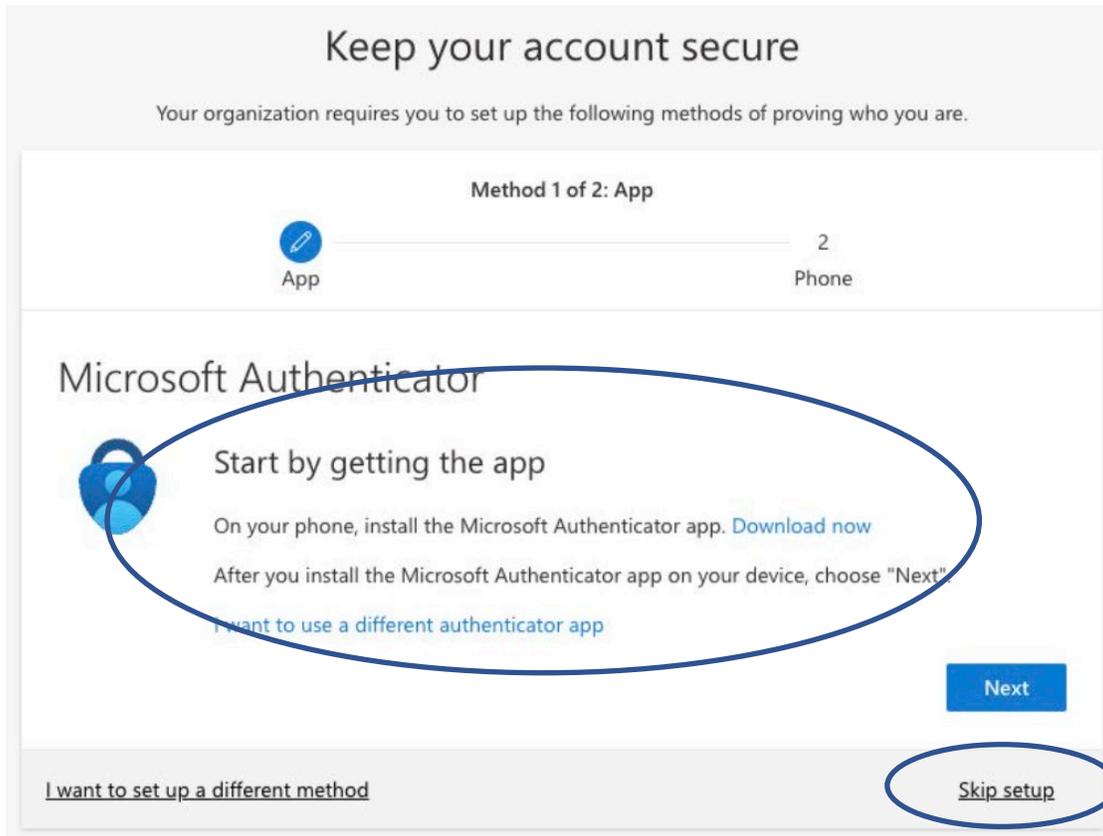


The screenshot shows the 'More information required' page. It features the Humber logo, the email address 'n01234567@humber.ca', the heading 'More information required', and the text 'Your organization needs more information to keep your account secure'. There are two blue links: 'Use a different account' and 'Learn more'. At the bottom right, there is a blue 'Next' button.

**Please Note:** Do not close this window as you will be returning to it after downloading the Microsoft Authenticator app.

## Choosing How to Set up Multi-Factor Authentication

There are three different ways to set up multi-factor authentication. In order of the preferred method, you can install the app and use the Microsoft Authenticator, you can set up using a mobile device, and/or you can set up using an email account. You will need to download the Microsoft Authenticator before getting started (explained in the next section). Leave this window open, as once the app has been installed, you will return to this window and click Next and scanning the QR Code with the Microsoft Authenticator app.



**Please Note:** If you choose **Skip setup**, you will not be offered this process again. But you can sign up by logging into [myaccount.humber.ca](https://myaccount.humber.ca)

## Downloading the Microsoft Authenticator App on your Phone or Mobile Device

- 1) Go to the App Store or Google Play and search for 'Microsoft Authenticator'. Install the app (with the icon of the lock as shown in the previous section). You will return to this window after you have finished installing the mobile app.
- 2) Open the mobile app and if prompted, allow for Authenticator to send you notifications. The window to **Add Account** should then open (Android users will have to skip a number of screens to get to this specific window). Click **Add Account** and the window asking what kind of account you are adding should appear. Select **Work or School Account**.
- 3) If prompted, allow the app to access your camera, as you will need to scan the QR code to add a new account. Click **Next** twice on the computer window – the QR code should be ready to scan. Once you have scanned the QR code, the authenticator app on your mobile should successfully add your account without requiring and additional information from you. Click **Next** on the computer window and then check your mobile and click **Approve**. The computer window will acknowledge the approval. Select **Next**.
  - a. **Please Note:** If the QR code reader on your phone can't read the code, you can select the **Can't scan the QR code link** and manually enter the code and URL into the Microsoft Authenticator app.

## Finish Setting up on Computer/Setting up a Different Method

Whether you are finishing up using the Microsoft Authenticator, or chose to set up with your mobile, you will do the following steps:

- 1) On the computer, choose the country, and enter your mobile phone number. Click **Next**.
- 2) A 6-digit code will be sent to your mobile. Enter that code on the computer and click **Next**.
- 3) You will receive notification that your SMS was verified and that your phone is now registered. Click **Next**.
- 4) Success! You will see a window informing you that you have successfully set up your security information. You will also see your phone and default information. Click **Done** to continue signing in.

The screenshot shows a web interface titled "Keep your account secure". Below the title, it says "Your organization requires you to set up the following methods of proving who you are." There are two options: "App" (with a green checkmark) and "Phone" (with a blue checkmark). The "Phone" option is selected. Below this, the "Phone" section is active. It says "You can prove who you are by answering a call on your phone or texting a code to your phone." and "What phone number would you like to use?". There is a dropdown menu for the country, currently set to "Canada (+1)", and a text input field containing "4162061317". Below the input field, there are two radio buttons: "Text me a code" (which is selected) and "Call me". At the bottom of the form, there is a blue "Next" button. At the very bottom of the page, there are two links: "I want to set up a different method" and "Skip setup".

The screenshot shows the same web interface as the previous one, but now the "Phone" section is further advanced. It says "We just sent a 6 digit code to +1 6473276579. Enter the code below:". There is a text input field for the code, and a "Resend code" link below it. At the bottom right of the form, there are "Back" and "Next" buttons. At the very bottom of the page, there are two links: "I want to set up a different method" and "Skip setup".

## Logging into Apps that Require MFA

If you are logging onto an application that uses MFA on your computer or phone, a window will appear asking for you to approve the sign in request. A notification will be sent to your phone. Open the Microsoft Authenticator app and approve the request. You can also indicate you want to use another option to receive a text or email.

## Changing your Notification Method

If you want to change your notification method, visit: [myaccount.humber.ca](https://myaccount.humber.ca). Click on **Security Info**, located on the left-hand menu. Select the **Change** link next to the **Default sign-in method** (at the top of the page). A drop-down box will appear with the options. Click on the method you want your default to be and select **Confirm**.

## Updating Your Settings

If you need to update your information, visit: [myaccount.humber.ca](https://myaccount.humber.ca). Click on **Security Info**, located on the left-hand menu. Select **Change** in the Phone area and update your mobile information. You will be sent a code to your phone to verify your identity.

## Help & Support

Please contact the I.T. Support Centre if you experience any issues.

Phone: 1 (416) 675-6622 ext. 8888

Web Chat: <https://humber.ca/techtalk>

Campus Location: A212 (Lakeshore) or Tech Zone – H109 (North)