

Overview

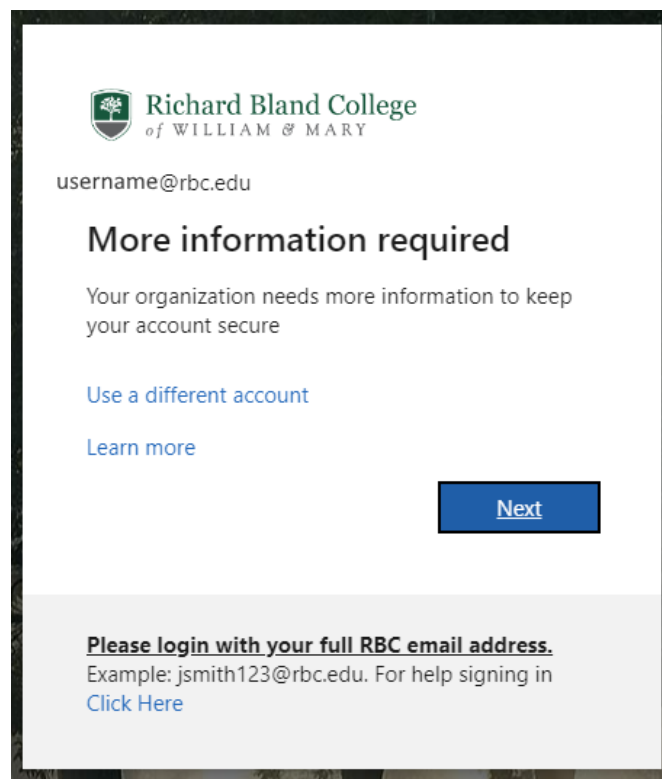
Multi-factor Authentication (MFA) is an **authentication** method that requires the user to provide two or more verification **factors** to gain access to resources such as online accounts, applications or VPNs. MFA is a core component of the RBC information security policy.

Multi-Factor Authentication works by requiring two or more of the following authentication methods:

- Something you know, typically a password.
- Something you have, such as a trusted device that is not easily duplicated, like a phone or hardware key.

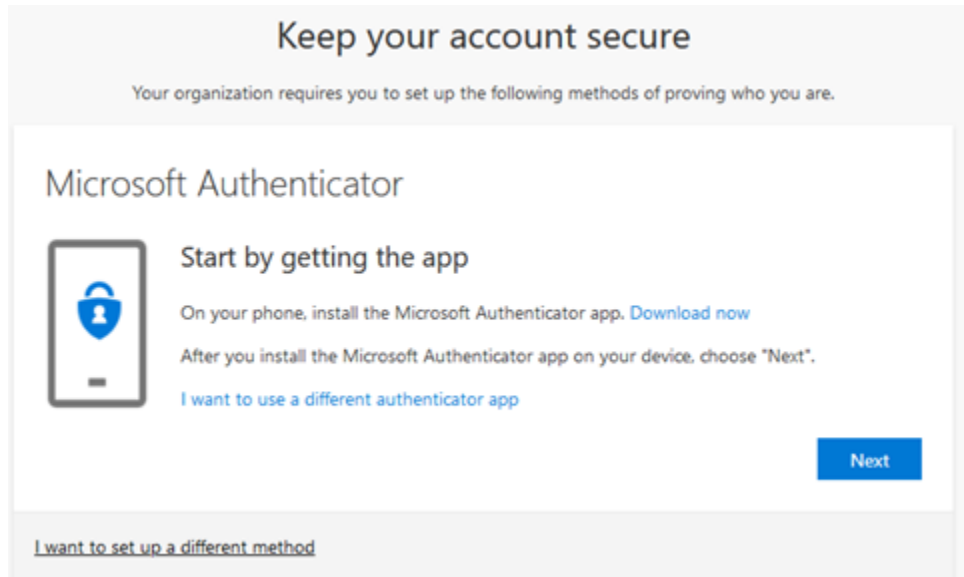
How to pre-register for MFA (Microsoft Authenticator App):

- 1.) Download the Microsoft Authenticator App to your cell phone.
- 2.) Browse to <https://aka.ms/mfasetup>.
- 3.) Log in with your Full RBC Email Address and password.
- 4.) You will be prompted with a notice for additional information.



5.) Click next and follow the on screen prompts to set up the app with your RBC Statesman account.

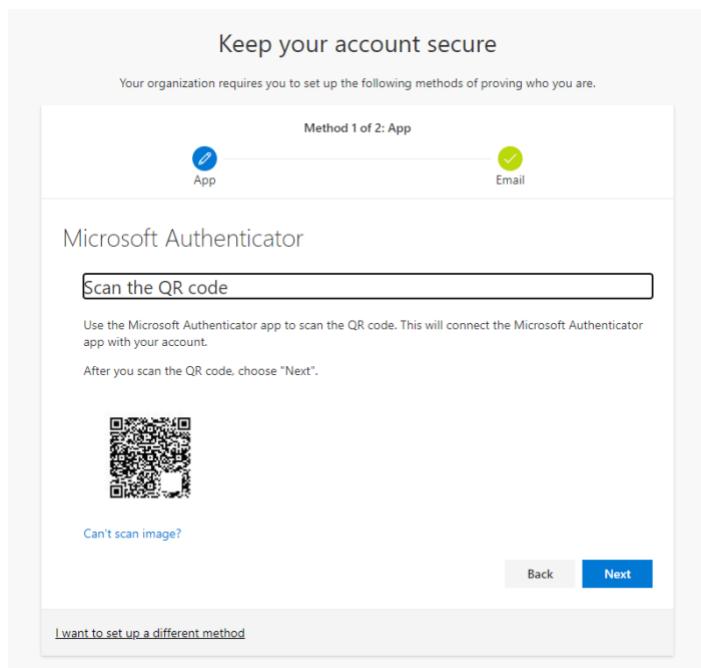
**If you want to use a method other than the Mobile App, you can select "I want to setup a different method" in the lower left hand corner of this screen. While text message, email and phone call are valid options, we strongly encourage the use of the mobile app as it presents a much more difficult target for malicious hackers.



6.) On your mobile device, open the Microsoft Authenticator app.

7.) Click the plus button and select "Work of School account".

8.) Scan the QR code displayed on your computer screen.




- 9.) At this point you will be prompted with the screen below, you will notice a number at the bottom, in our example the number is “40”. You should receive a prompt on your mobile device asking you to enter the number displayed on the screen. Enter the number now.

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Microsoft Authenticator



Let's try it out

Approve the notification we're sending to your app by entering the number shown below.

40

BackNext


[I want to set up a different method](#)


- 10.) If you correctly entered the number you will get the following notifications and you have successfully setup Multi-Factor Authentication! Congratulations.

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Microsoft Authenticator



 Notification approved

BackNext

[I want to set up a different method](#)

Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Success!

Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method:



Microsoft Authenticator

Done

If for any reason you were unable to complete the steps as laid out here, feel free to reach out to the helpdesk. You can reach the IT Help Desk on campus ext. 6119 or off campus (804) 862-6100 ext. 6119.