



UPDATING USER CREDENTIALS/ MULTI FACTOR AUTHENTICATION (MFA) GUIDE



Contents

Updating User Credentials..... 3

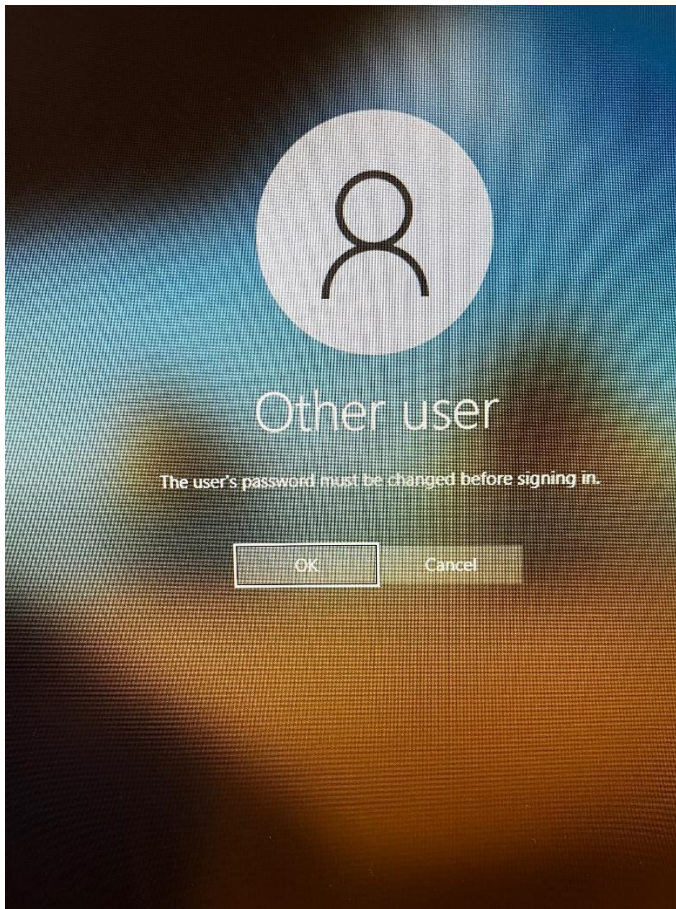
Multi Factor Authentication (MFA) Guide – app 4

Multi Factor Authentication (MFA) Guide – phone 11

Questions? 19

Updating User Credentials

1. When logging into a GC computer, you will be prompted to change your current password to one that meets the updated credential criteria:

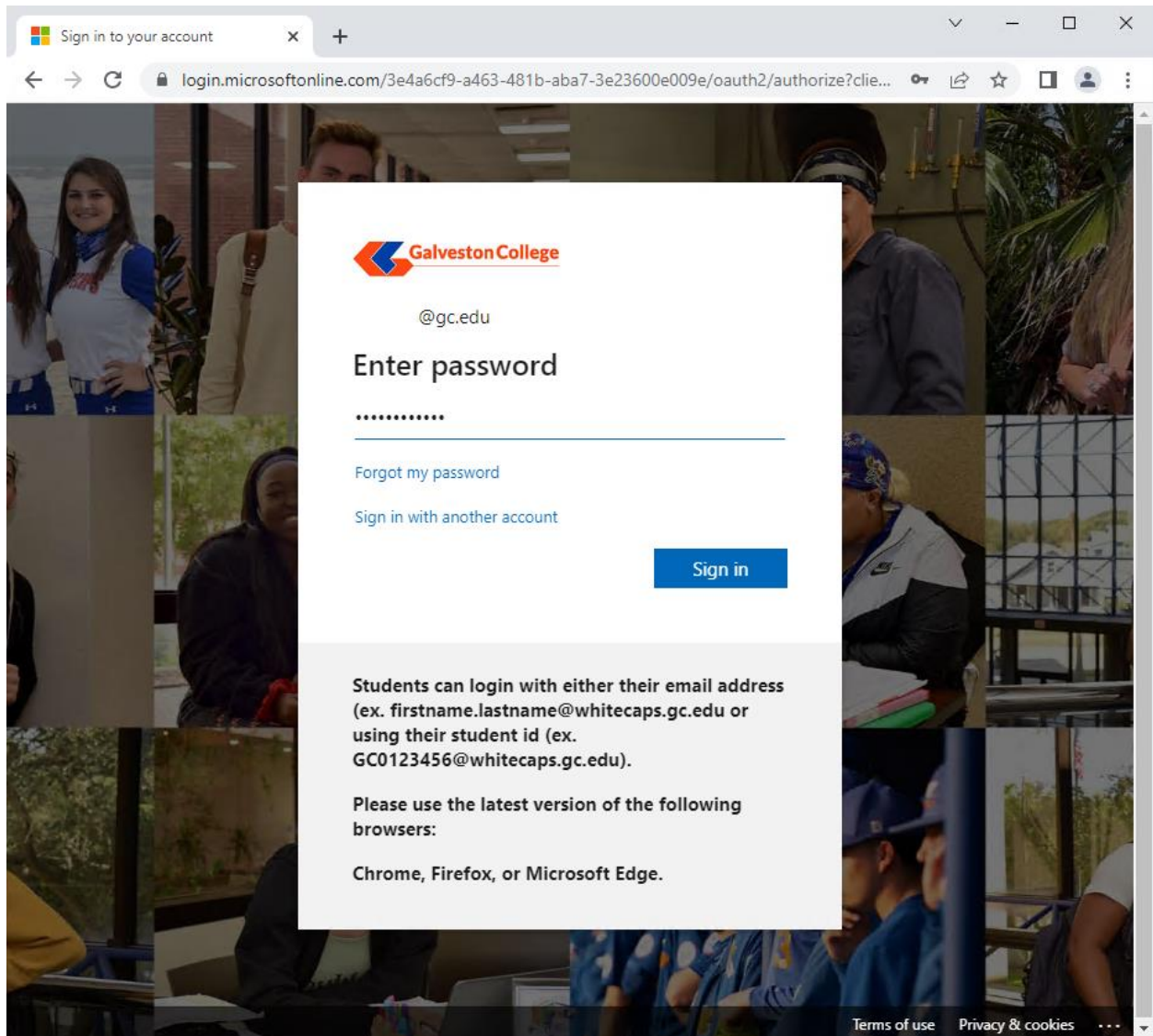


A passphrase is recommended versus a password as they are easier to remember and will allow you to easily fulfill the character length requirement. Updated credential criteria:

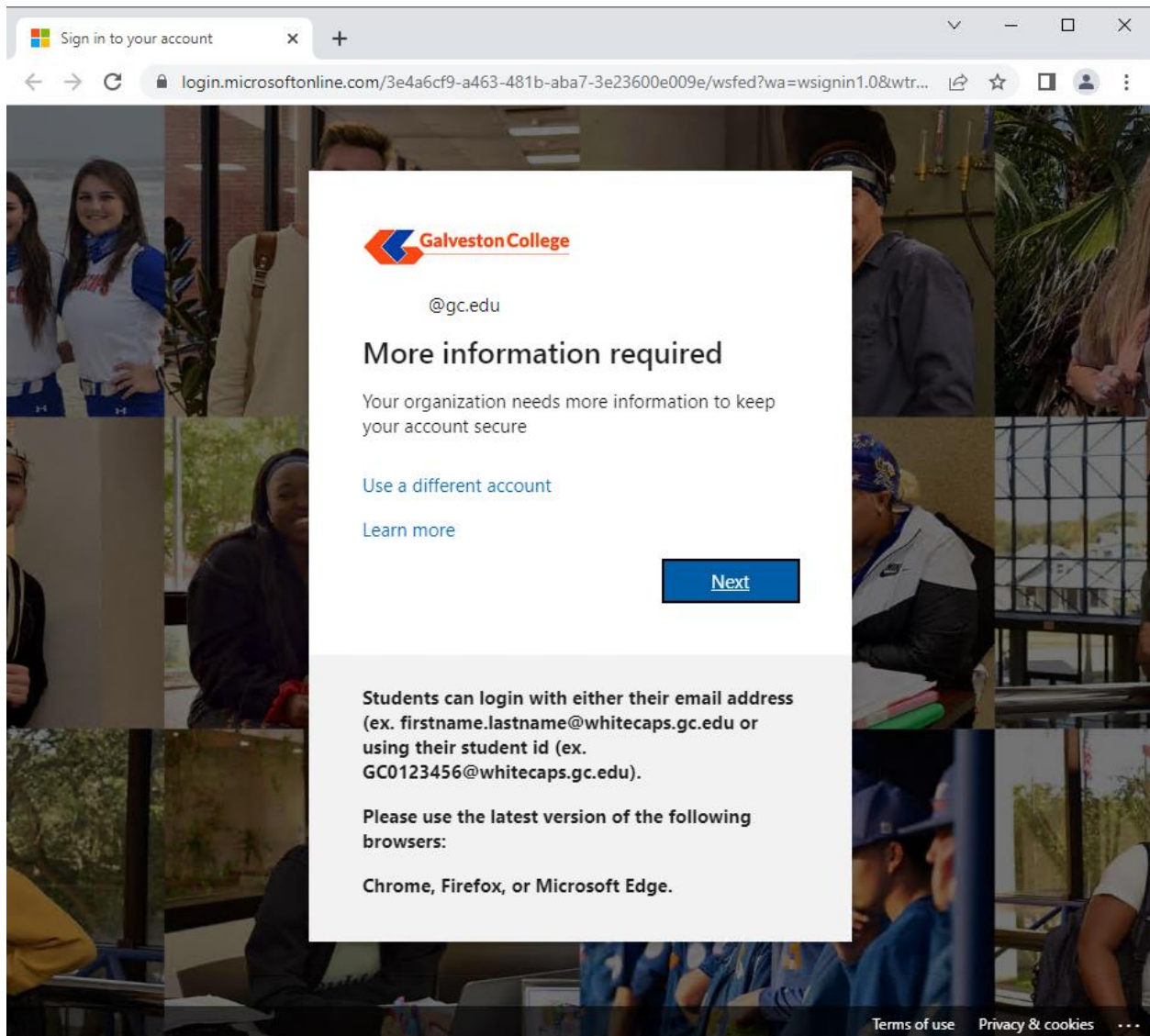
- Minimum password length: 15 characters
- No complexity rules
- Maximum password age: 365 days

Multi Factor Authentication (MFA) Guide – app

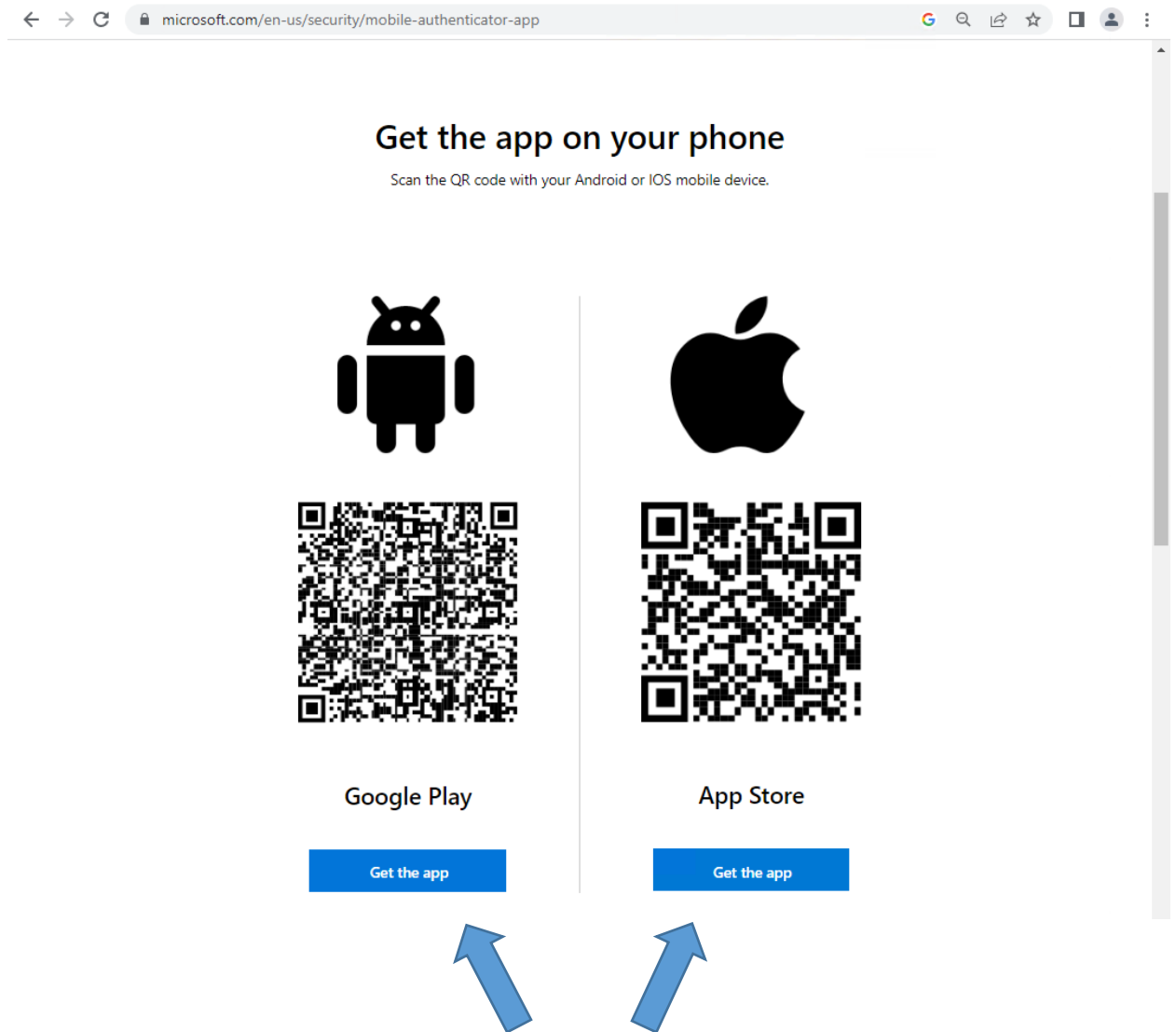
1. When attempting to access one of the applications that support MFA, you will be prompted to provide your credentials to begin the authentication process:



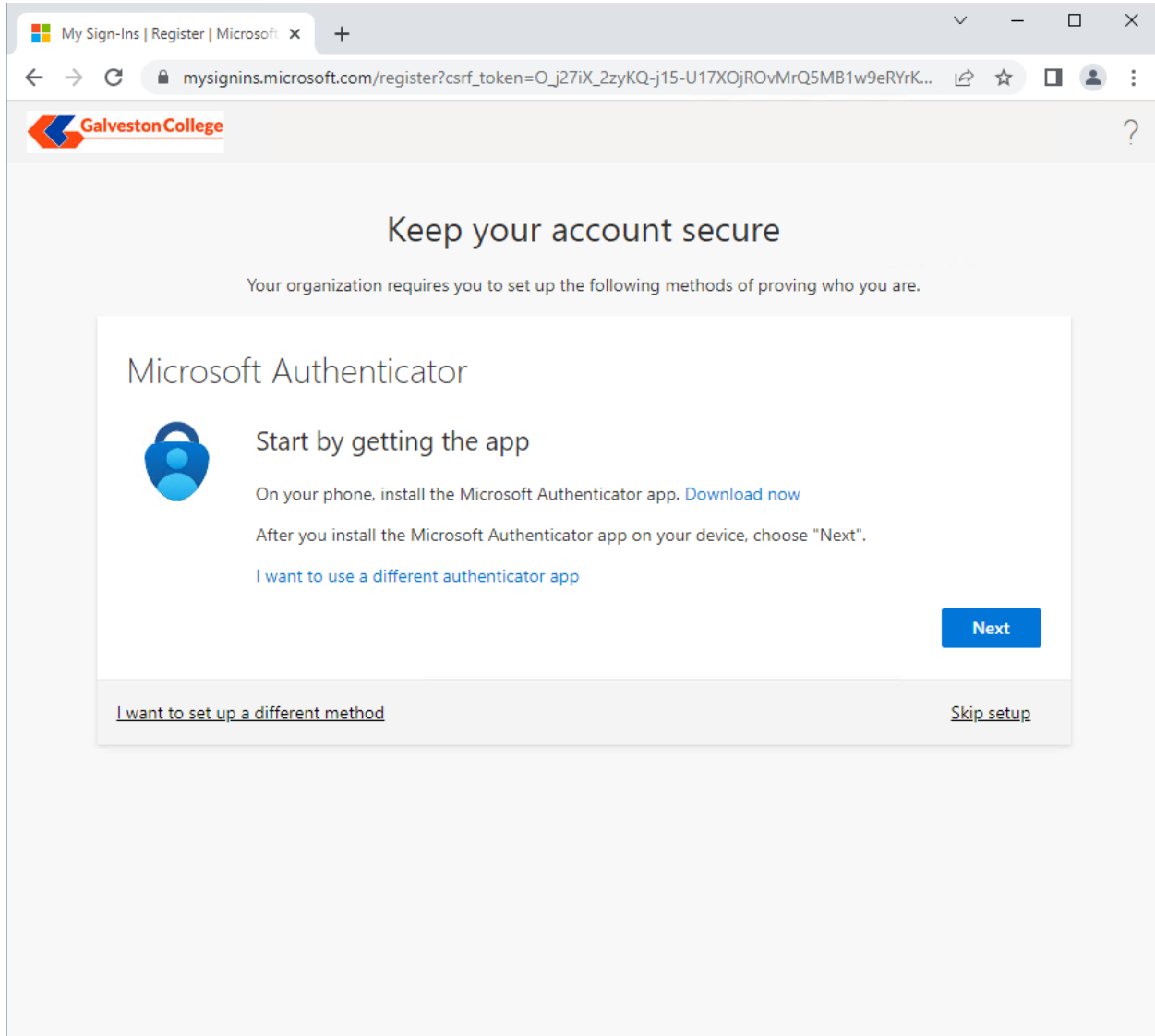
2. After providing the correct credentials, a screen will display informing you that additional information is needed:



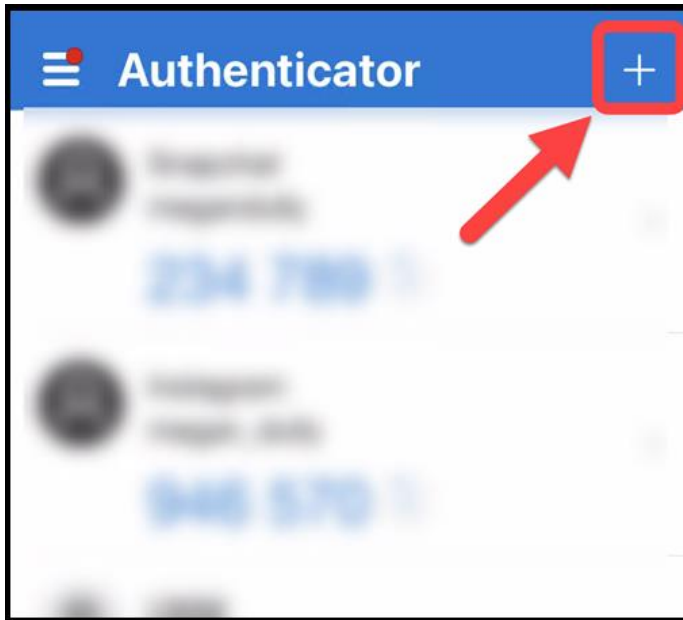
3. After clicking on next in the previous step, you will be asked to install the Microsoft Authenticator app. The screenshot below has been provided for your convenience to access the application and begin your download:



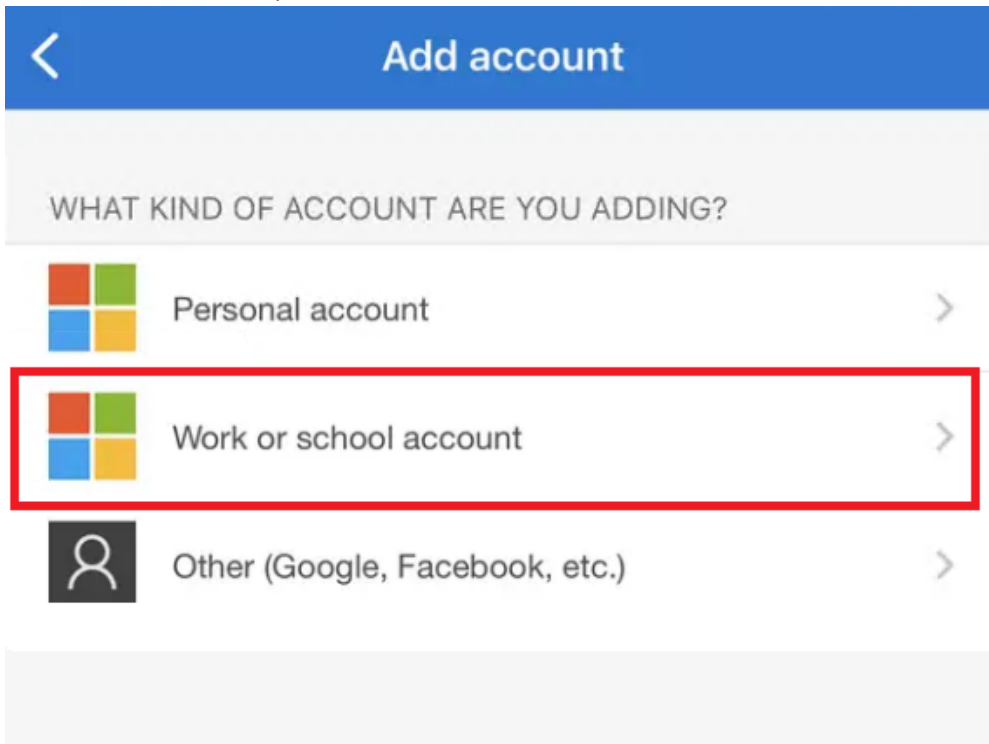
4. You can also select “I want to use a different authenticator app” if you currently have another authentication application you would prefer to use for your work account. After an authenticator application has been installed on your device, click next on the window to continue with the set up:



5. If using Microsoft Authenticator, click on the add account button on the top right of the application indicated by a white plus sign to add your account.



6. Select “Work or school account” when prompted to specify what type of account you are adding to the authenticator. Input the credentials you use to log into your computer and click next to continue with the setup:



- Using your phone or other device, scan the QR code that is provided to you to pair the device to your account. If you cannot see the QR code or are not able to scan it, click on the “Can’t scan image?” button located under the QR code. This will provide you with a URL and code combination needed to pair your mobile device to your account:

My Sign-Ins | Register | Microsoft

mysignins.microsoft.com/register?csrf_token=nalZcuL9lxQ2CsK434NcL6E6Ok9g--idE42XWv_27s...

Galveston College

Keep your account secure

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

Microsoft Authenticator

Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

After you scan the QR code, choose "Next".

[Can't scan image?](#)

Enter the following into your app:

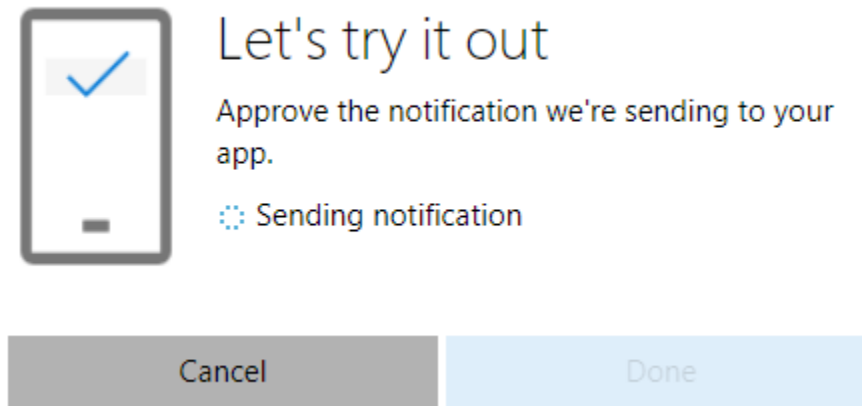
Code: 534501600

URL: <https://mobileappcommunicator.auth.microsoft.com/activate/369952595/EUS>

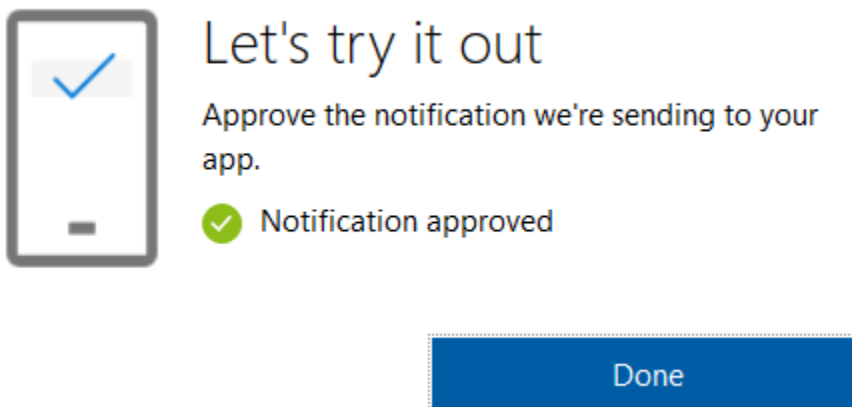
[Back](#) [Next](#)

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

- Next you will see a “Let’s try it out” window on your computer, click next. A notification will be sent to your mobile device via the Microsoft Authenticator app. Once you receive the notification in the app, press “Approve”. This action confirms that you are attempting to log in.
-

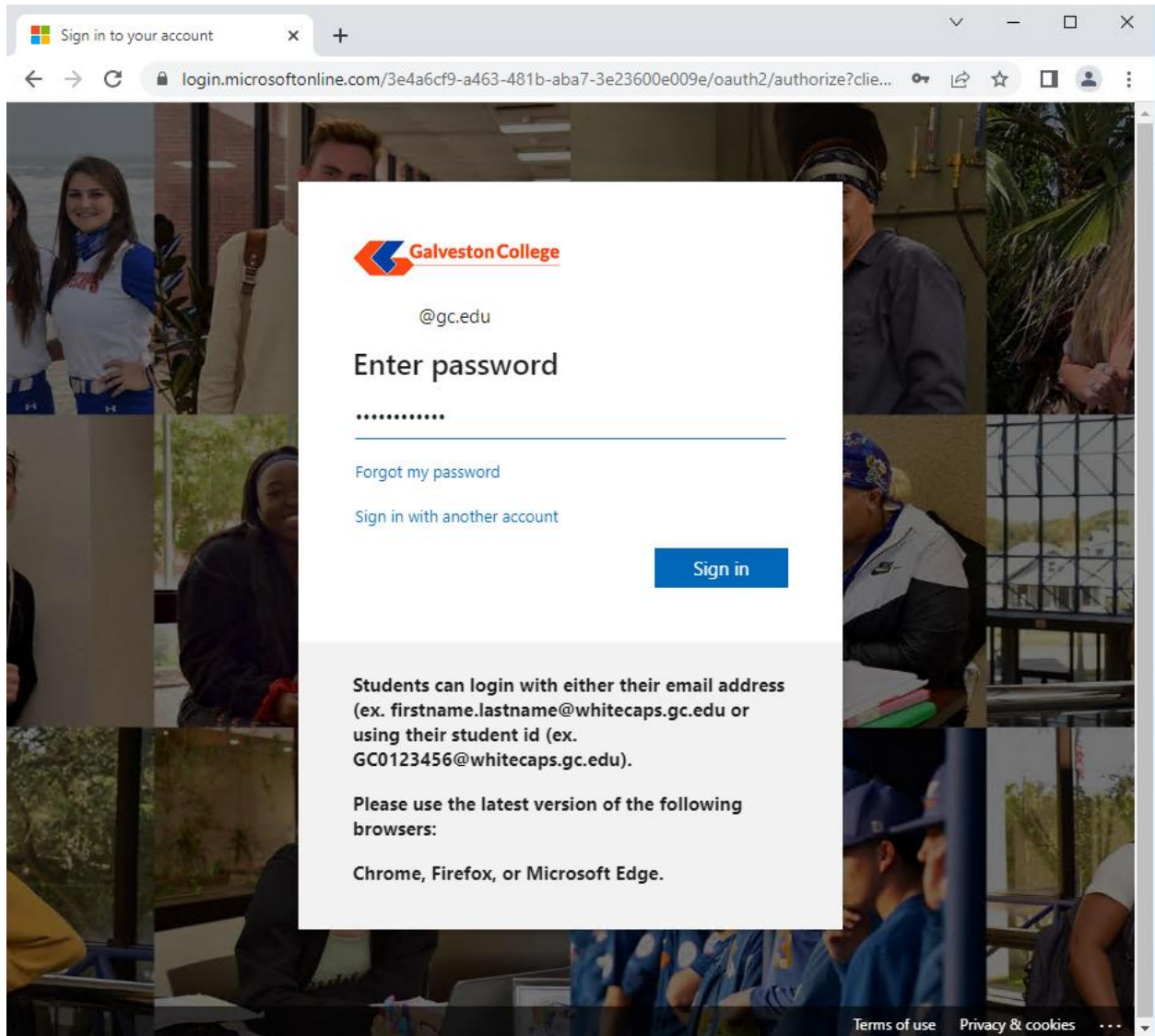


- Once the connection is successful, the screen on your computer will show that your notification was approved by displaying a green check mark.

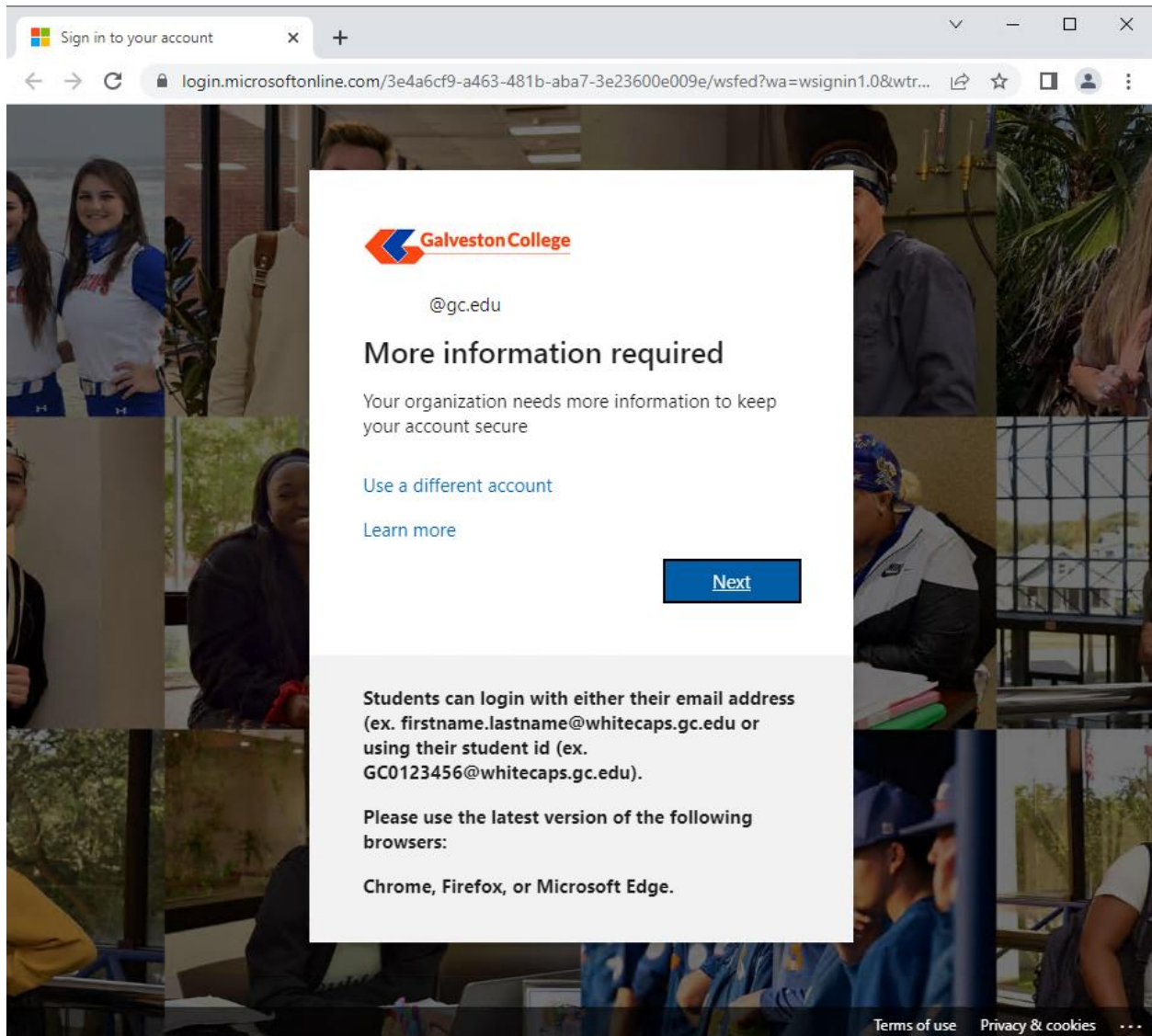


Multi Factor Authentication (MFA) Guide – phone

1. When attempting to access one of the applications that support MFA, you will be prompted to provide your credentials to begin the authentication process:




2. After providing the correct credentials, the next screen will indicate that additional information is needed. Click next.



Sign in to your account

login.microsoftonline.com/3e4a6cf9-a463-481b-aba7-3e23600e009e/wsfed?wa=wsignin1.0&wtr...

 Galveston College

@gc.edu

More information required

Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

Next

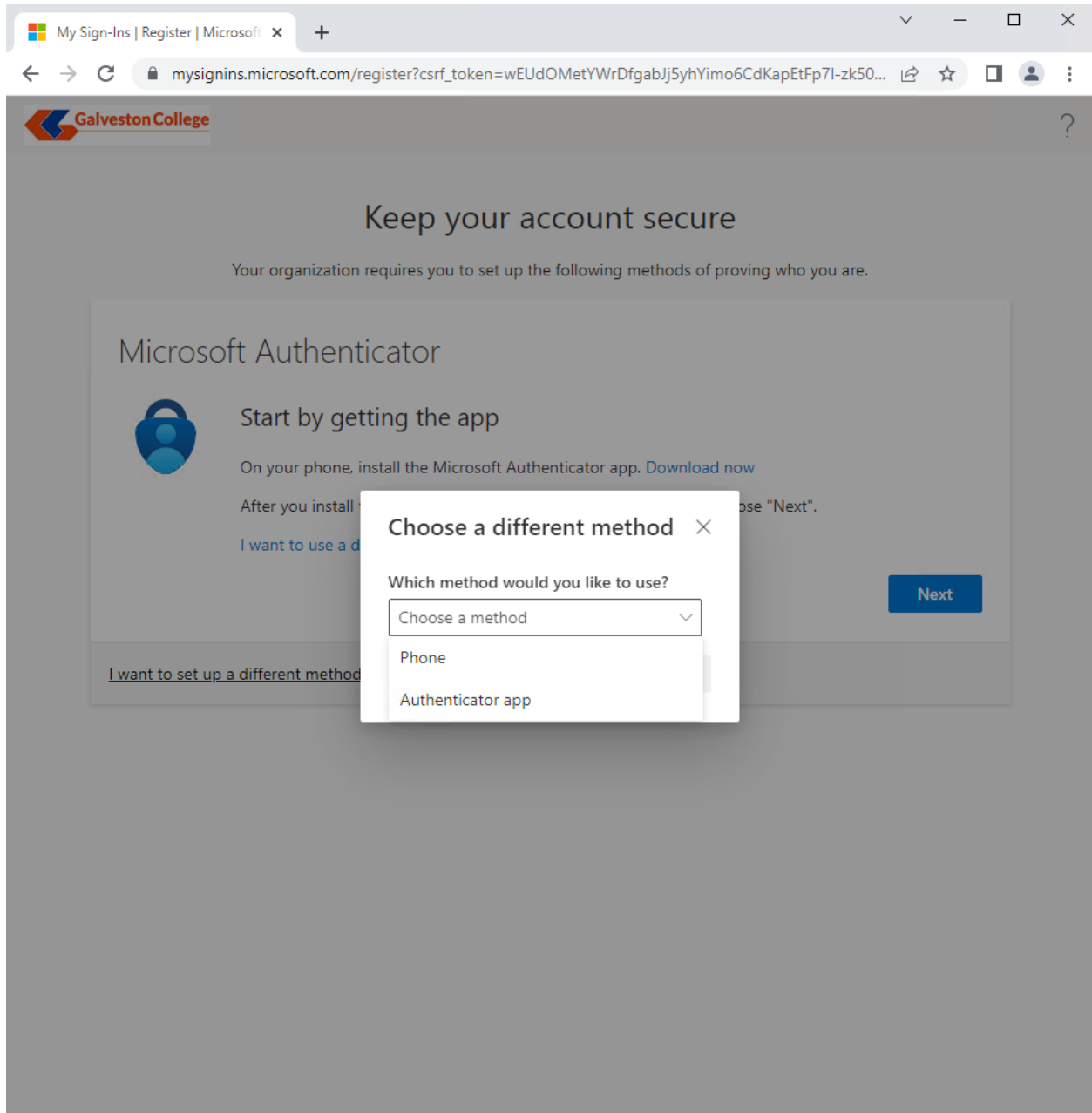
Students can login with either their email address (ex. `firstname.lastname@whitecaps.gc.edu` or using their student id (ex. `GC0123456@whitecaps.gc.edu`).

Please use the latest version of the following browsers:

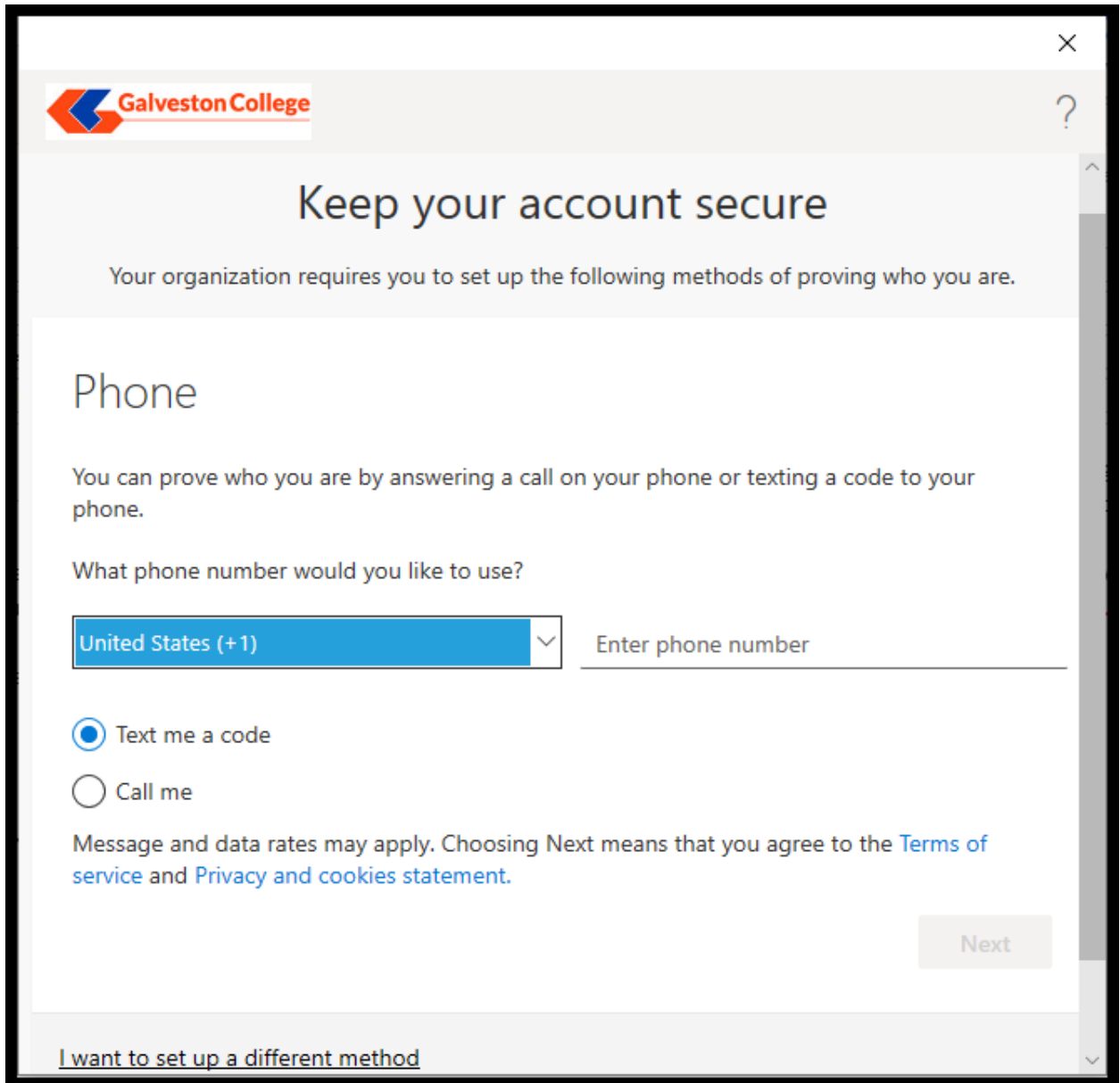
Chrome, Firefox, or Microsoft Edge.

[Terms of use](#) [Privacy & cookies](#)

3. You then will be prompted to install the authenticator app or you can select “I want to set up a different method” to skip the app installation process. You will be provided with a drop-down menu listing the phone option. Select phone and click next:



4. Input your phone number and select how you would like to be reached, via text or phone call:



The screenshot shows a web browser window with the Galveston College logo in the top left corner. The main heading is "Keep your account secure". Below the heading, a message states: "Your organization requires you to set up the following methods of proving who you are." The section is titled "Phone". A sub-heading reads: "You can prove who you are by answering a call on your phone or texting a code to your phone." The question "What phone number would you like to use?" is followed by a dropdown menu showing "United States (+1)" and a text input field labeled "Enter phone number". There are two radio button options: "Text me a code" (which is selected) and "Call me". A note at the bottom of the form says: "Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#)." A "Next" button is located at the bottom right of the form area. At the very bottom of the window, there is a link: "[I want to set up a different method](#)".

5. If you opt for the text option, a message will be sent to your phone containing a 6-digit code. Input the code in the box and click next:

My Sign-Ins | Register | Microsoft

mysignins.microsoft.com/register?csrf_token=wEUdOMetYWrDfgabJj5yhYimo6CdKapEtFp7I-zk50...

Galveston College

Keep your account secure

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

Phone

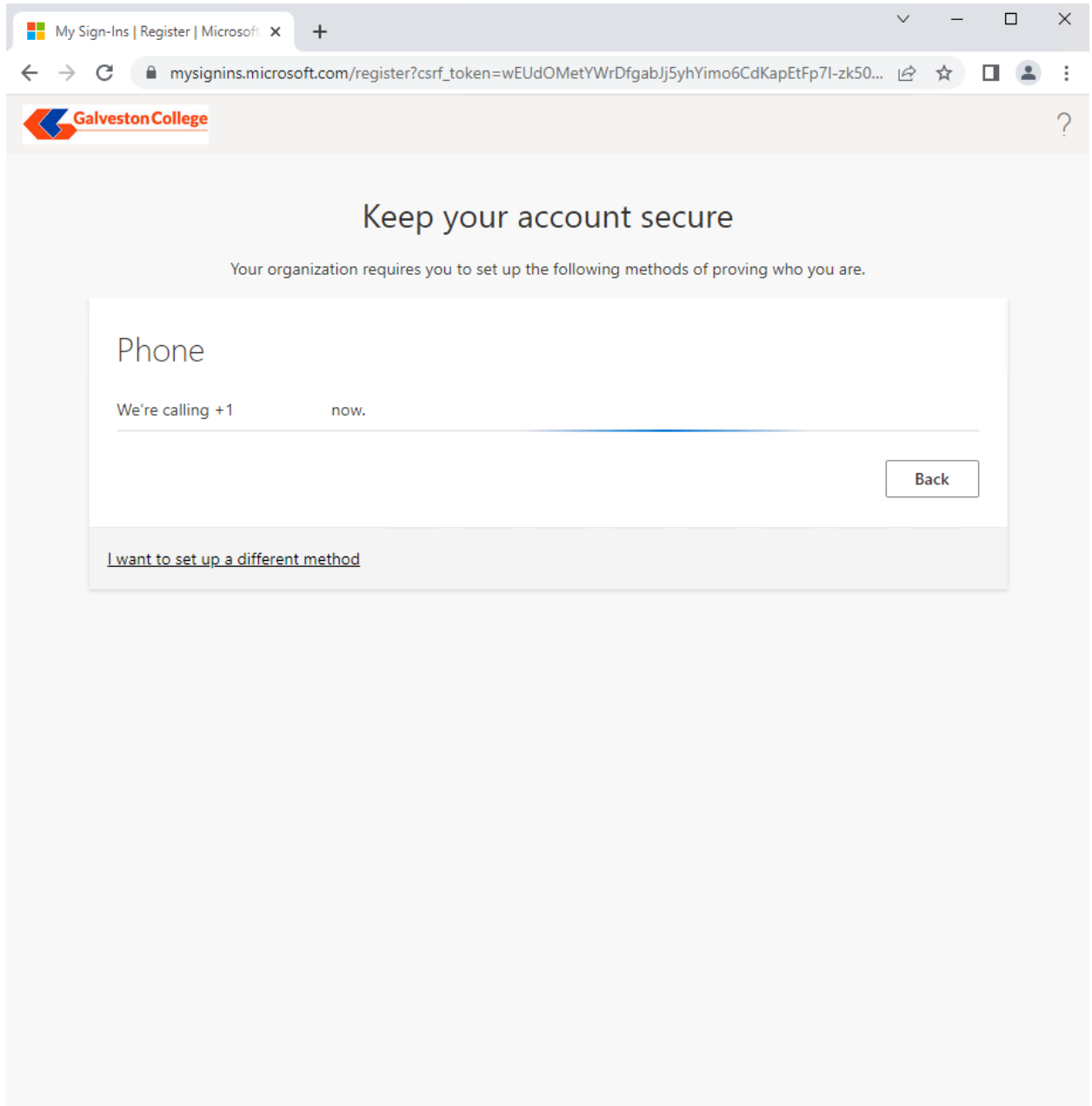
We just sent a 6 digit code to +1 . Enter the code below.

[Resend code](#)

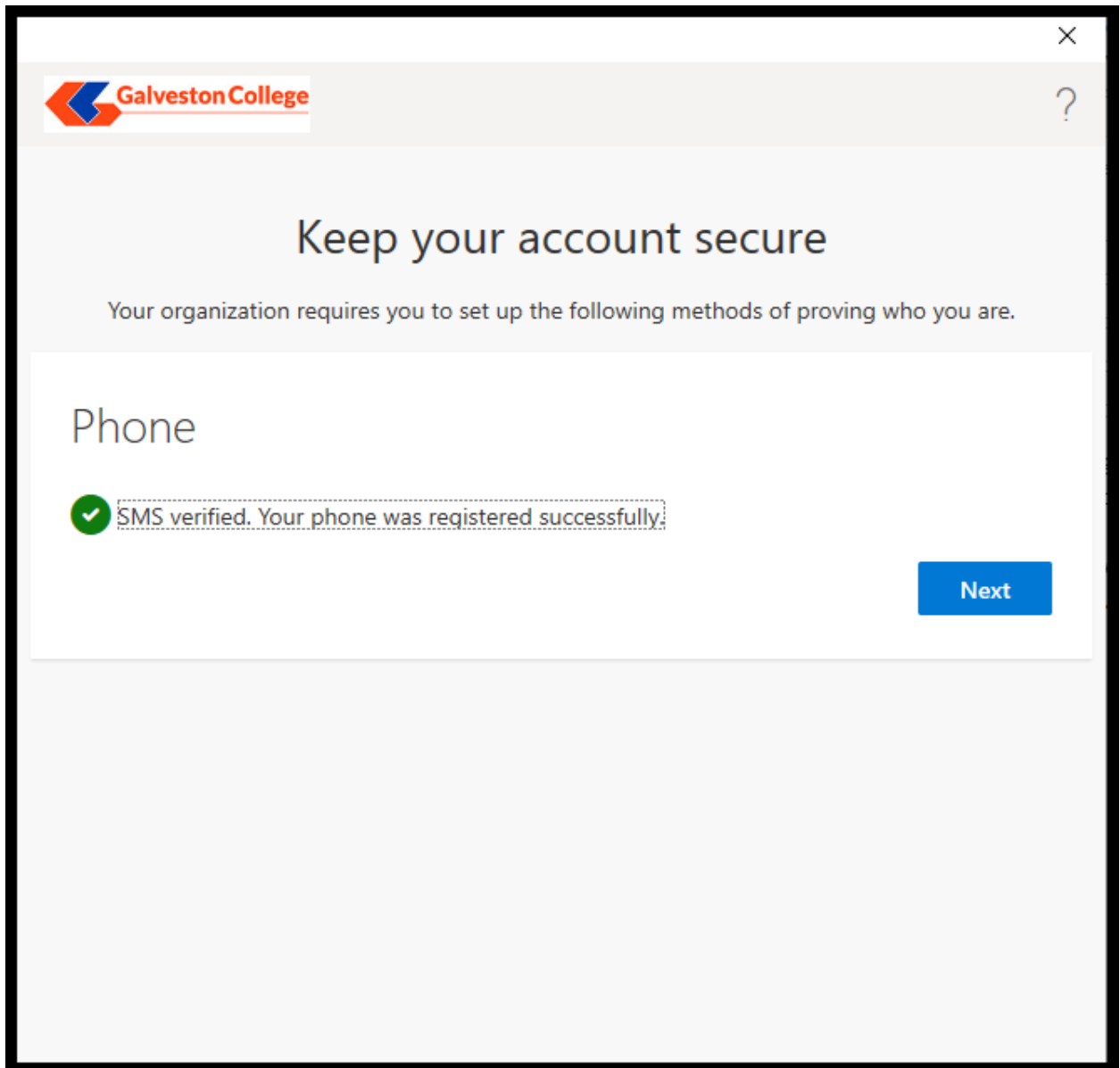
[Back](#) [Next](#)

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

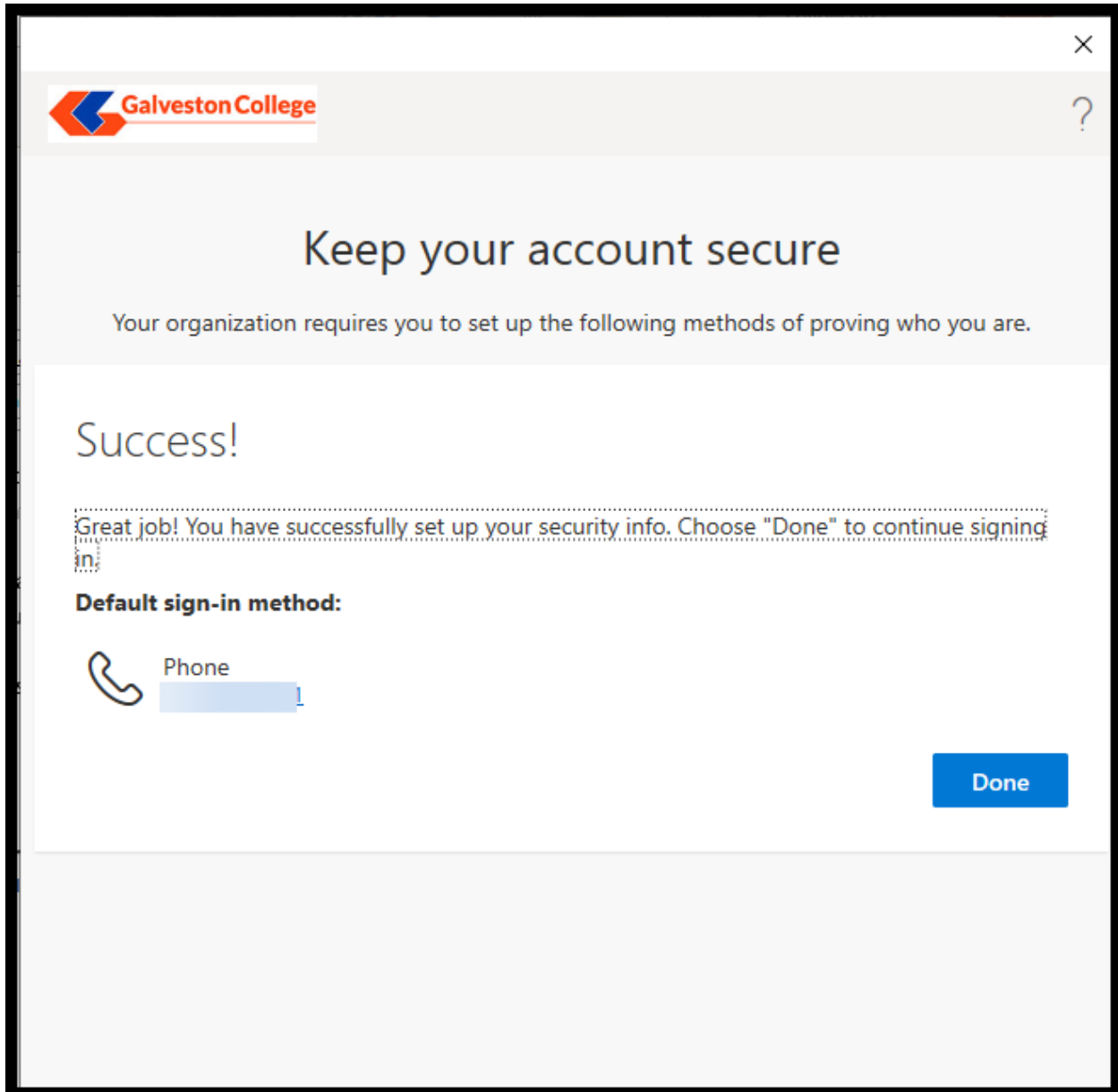
6. If you opt for the call option, a phone call will be made to your phone. Answer the call and follow the prompts to confirm you are attempting to authenticate:



7. After you verify your phone, a message will appear on your computer with a green check mark confirming that you are registered for MFA. Click next to continue with the set up:



8. A final message will appear displaying the phone utilized to set up MFA. Click done to continue signing in:



The screenshot shows a dialog box with a light gray header containing the Galveston College logo and name on the left, and a close button (X) and a help button (?) on the right. The main content area has a white background and contains the following text: "Keep your account secure" in a large font, followed by "Your organization requires you to set up the following methods of proving who you are." Below this is a "Success!" message, a dashed-line bordered box containing the text "Great job! You have successfully set up your security info. Choose 'Done' to continue signing in.", and a section titled "Default sign-in method:" with a phone icon and the word "Phone" next to a blue input field. A blue "Done" button is located in the bottom right corner of the dialog box.

Questions?

If you have any questions regarding the new password policies or the MFA process, please contact the IT Service Desk via the following methods:

- Phone: 409-944-4242
- Email: servicedesk@gc.edu