MULTI-FACTOR AUTHENTICATION

Step-by-step instructions for setting up multi-factor authentication for your Office 365 account.

Multi-factor Authentication (MFA) is a two-step process, that requires users to enter their password (step 1) and then verify their identity using an additional method (step 2), when performing account sign-in transactions from off campus. MFA adds a vital layer of security needed to protect accounts from ever increasing instances of phishing attempts and password hacks.

Once MFA is enabled for your account, you must first set up at least two additional verification methods (for the first method you must choose either the authenticator app or phone – text or call, and for the second method you can use the method you didn’t choose above or a personal non-CofC email address). It is best to set up multi-factor authentication additional verification methods from a desktop computer while on campus.

STEP 1:

To set up your additional verification methods, log in to portal.office.com with your College of Charleston credentials. A window will pop up saying that more information is required. If your email address is already displayed in this window, click Next. If it is not displayed, enter your complete email address, then click Next.

STEP 2:

On the next window, you will see two verification methods listed, authenticator app and phone. If you would like to use the methods shown, proceed by clicking Set up and skip to Step 4. If you would like to change the methods shown, click Choose security info and proceed to Step 3.
**STEP 3:**

On this window you can change your verification methods. For example, the authenticator app is listed as your first method, but you would rather use a phone number as your first method, you can change that here. To do this, change the Second Method from phone to email first, then change the First Method from authenticator app to phone. Once you change your methods, click **Close**.

**Choose security info**

```
FIRST METHOD
Authenticator app

SECOND METHOD
Phone
```

**STEP 4:**

If you chose the **authenticator app** as a verification method, install the Microsoft Authenticator app on your Android, iOS (you may need your Apple ID and Password), or Windows Phone at https://www.microsoft.com/en-us/account/authenticator. In the app, on the Accounts screen, select **Add account**. Then, select **Work or school account** and scan or manually enter QR code displayed on your desktop computer screen.

If you chose **phone** as a verification method, click **Set up**.
Then, select United States from the drop down menu. Then, enter the phone number of the device you prefer to verify with. This is typically your cell phone. Next, you can choose to verify with a code that is texted to you or by answering a call and pushing # to confirm your identity. Click Next to continue.

Depending on what you selected, you will either receive a code by text or a phone call. If you chose Text me a code, enter the code and click Done. If you chose Call me, answer the call and push # to confirm your identity.

If you chose email as a second verification method, enter the personal non-CofC email address you prefer to verify with. Click Next to continue.

**STEP 5:**

Once you are finished setting up your additional verification methods, choose Done. Now that set up is complete, the next time you perform an account sign-in transaction from off campus, you will be prompted to verify your identity using an additional method.

For questions, contact the Helpdesk by email helpdesk@cofc.edu, chat help.cofc.edu, or phone 843.953.3375.