What is Two-Factor Authentication?

Two-factor authentication is a way of providing greater security to your logins. Instead of providing just a username and password to login to a web site, you can enable two-factor authentication which requires you to provide an additional PIN code from your mobile phone thereby increasing security (requiring 'something that you have' as well as 'something that you know'). This PIN code can be supplied by a mobile app that has been configured with your account. It does require you to be in possession of your mobile phone to login to your CUE account but provides a significant improvement to the security of your CUE account.

How do I set it up?

Two-factor authentication can be enabled on your account in Online Services under the Change Password page: https://onlineservices.concordia.ab.ca/
A complete MFA set-up guide is available here.

You will be presented with these options:

1) Using a mobile app
2) Hardware key

CUE IT Services recommends the Google Authenticator app, which is available for Android in the Google Play Store and iOS through the iTunes store. The hardware key option uses a physical USB device that needs to be plugged in to the device that you are logging into.

More information can be found on the following document:

- Two Factor Authentication with Mobile App