Wharton County Junior College

What is Multi-Factor Authentication (MFA)?

MFA, also referred to as two-factor authentication, is a method of system access control in which a user is only granted authorization after successfully providing a second authentication method beyond the basic username/password. A user is required to enter a password and also authenticate using a second factor, typically a cell phone or personal email address (to receive a verification code).

The concept is based on:

- Something you know – your MyWCJC username and password
- Something you have – your mobile phone and/or alternate email addresses

Benefits

- Prevents unauthorized access to your information
- Protects College data, even if a MyWCJC username and password have been compromised
- Helps identify compromised credentials before they are misused
- Provides options for your second authentication factor (phone or email)

What Triggers MFA

- MFA stores a number of factors for your device, such as IP address, browser version and location. If any of these factors change, you will be prompted to re-verify your device. Click "Trust this device" if you are using a private device. Never “Trust” a public device.

What Happens When MFA is Triggered

- You will be required to answer one of your pre-set security questions.
- You will be sent a verification code to your alternate email or cell phone. Verification code must be entered into your device within 30 seconds.
- Don't forget to click "Trust this device" if you are using your personal device.