



Multi-factor Authentication

Multi-factor authentication (MFA) is a security layer that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.

Your credentials fall into any of these three categories: **something you know** (like a password, PIN#, DOB), **something you have** (like a smart card or one-time passcode), or **something you are** (like your fingerprint). Your credentials must come from two different categories to enhance security – so entering two different passwords would not be considered multi-factor.



An example of Multi-factor authentication is the website you are logging into sending a code to your email or cell phone to log into your account.

Why MFA?

The goal of MFA is to create a layered defense which makes it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database.

MFA helps protect you by adding an additional layer of security, making it harder for hackers to log in as if they were you. Your information is safer because thieves would need to steal both your password and your phone. You would notice if your phone went missing, so you'd report it before a thief could use it to log in. Plus, your phone should be locked, requiring a PIN or fingerprint to unlock, rendering it even less useful if someone wants to use your MFA credentials.

When should I use MFA?

You should use MFA whenever possible, especially when it comes to your most sensitive data—like your primary email, your financial accounts, and your health records.



OET Information Security:
Sylvester Lee
sylvester.lee@ggc.edu
678-407-5439

