UMIT PRESENTS

Made for U

At a glance:

As you may know, University of Miami Information Technology (UMIT) implemented an important security feature called Multi-Factor Authentication (MFA) over the summer.

We understand that utilizing MFA may take some getting used to, but having a second factor (e.g., mobile phone or landline) in addition to your CaneID credentials is far more secure than your username and password alone. Since hackers don't have physical access to these devices while attempting to compromise your account, your information is secure.

Have questions? Get answers:

For answers to common questions and troubleshooting support, please review MFA's frequently asked questions.

Learn more about MFA:

Review all MFA documentation at: miami.edu/multifactor.

Who to contact:

If you have any questions about MFA, please contact the UMIT Service Desk at: (305) 284-6565 or itsupportcenter@miami.edu.

Multi-Factor Authentication

Important Tips & Resources

In order to facilitate a seamless authentication process with Duo MFA, below are a few important tips and resources:

Using the same device? Use the "Remember Me" option.

- After logging in with your CaneID and password, you will be prompted for MFA verification. Check the box "**Remember me for 30 days**" before choosing a verification method. You will be remembered on that device and browser, and you will not need to confirm your identity with MFA verification again for 30 days.

Traveling with MFA is easy!

- If you are traveling outside the country, and/or don't have access to an Internet connection and/or phone service, you can still use MFA. If you don't have Internet, you can elect to receive an SMS text or a phone call to verify your authenticity. If you don't have phone service, you can select the key symbol on the mobile app screen and generate a passcode. View our MFA traveling tips guide for more details.

MFA works with or without a smartphone.

- It is highly recommended that you use the Duo Mobile app or generate a passcode, but you don't need a smartphone to use MFA. You can use a landline, a standard cell phone, or tablet. A hardware token may also be used to authenticate.

- There are also various ways to authenticate your login with MFA. For more information, review our authentication prompt guide.

Register two or more devices with MFA.

2+

- It is recommended that you register at least two devices, for example, both a smartphone and an office phone. That way, if you don't have your smartphone on you, you will still be able to access protected systems using your secondary device.

- For step-by-step instructions, review our adding a new device or adding a new device when you have "automatic push" enabled guides.

- If you would like to manage your devices or replace a device (such as remove your old cell phone and add a new one), please review our managing your existing devices guide.

View all available services and products at:

it.miami.edu

MIAMI INFORMATION TECHNOLOGY