

Account Management FAQ

Click any of the Frequently Asked Questions (FAQs) to jump to the answer.

[What is MFA?](#)

[What is 2FA?](#)

[Why is MFA Necessary?](#)

[What verification options are available?](#)

[How does each verification method work when signing in?](#)

[I forgot my password. How do I get back into my account?](#)

[What makes a good password?](#)

[Can I opt out of MFA?](#)

What is MFA?

Multifactor authentication or MFA is just a better way to make sure it's really you signing onto your Delta account. We do this by asking for two or more kinds of proof.

These types of proof, also called factors, are:

- Something you **know**, like a password or PIN #.
- Something only you **have**, like a smartphone
- Something you **are**, like your fingerprint.

At Delta College, you'll typically be asked to provide your password and prove you have a device with you, like your smartphone.

When you enroll in MFA, you'll choose some **verification methods** that work for your situation.

See the "[What verification options are available?](#)" section for more details.

[\(Top\)](#)

What is 2FA?

Two-Factor Authentication or 2FA is just another term for Multifactor Authentication (MFA). 2FA refers to needing two forms of proof. MFA refers to needing two or more forms of proof. You can use either term and we'll know what you mean.

[\(Top\)](#)

Why is MFA necessary?

The internet bad guys are very good at tricking us. It's their job to think of ways to hack into accounts and trick people into accidentally giving out their information.

Sometimes the bad guys use lies and tricks in emails, called phishing, to get you to enter your username and password into their fake website. If only a username and password is needed, they can take over your account and pretend to be you. There are several ways they can make money by taking over your account, so they will keep trying. Their tricks are getting more believable every day making it easier for the rest of us to make mistake.

Your Delta account is very important communication tool. It also provides you access to your personal information, academic records, and payment information. It must be carefully guarded to protect you from identify theft and other forms of fraud.

Delta College also must adhere to several sets of rules required by federal & state government entities, its accrediting organization and financial institutions.

[\(Top\)](#)

What verification options are available?

When signing onto a Delta College electronic resource you will be asked for your password and one other verification method.

When resetting a forgotten password you will be asked for two verification methods.

- This two-step process is referred to as Multifactor Authentication, or MFA.
- MFA helps secure your account from unauthorized access.

You must enroll in at least one preferred verification method and two total verification methods. We recommend enrolling in as many verification methods that work for your situation.

Preferred Verification Methods - May be used for Sign-On or Password Reset

You may enroll in any or all of the following verification methods, which can be used when signing on or resetting a forgotten password:

- **Phone:** Receive a call or verification code sent via SMS/Text message.
- **Alternative Phone:** Receive a call or verification code sent via SMS/text message.
- **Microsoft Authenticator App:** Receive an application notification or retrieve a verification code on a smart phone or tablet.
- **MFA Token:** If you do not have a mobile phone or tablet, contact the OIT Helpdesk and ask to be issued an MFA Token. There is no cost to you.

Refer to the table below to see what preferred verification methods can be used with each type of device you may have.

Devices	Preferred Verification Methods Supported				Uses	
	Call	SMS/Text	App Notification	App Code	Sign-on	Password Reset
Home or Office Phone	X				x	x
Basic Mobile Phone	X	X			x	x
Smart Phone	X	X	X	X	x	x
Tablet			X	X	x	x
MFA Token				X	x	x

Optional Verification Methods - May be used for Password Reset Only

You may also enroll in any or all of the following verification methods, which can be used for resetting a forgotten password:

- **Security Questions:** Set up a bank of 5 security questions. 3 of 5 are randomly selected when used.
- **Alternative Email:** Receive a verification code sent to a non @delta.edu email.
- Enroll any of the following devices and use their supported verification methods as a way to verify your identity when signing in.

[\(Top\)](#)

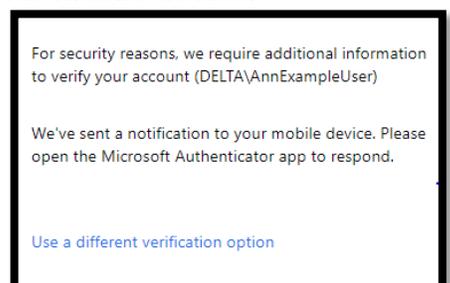
How does each verification method work when signing in?

After entering your username and password, the sign-on screen will indicate which method it is trying to use to confirm your identity. If you want to use a different method to verify, click the link that says “Use a different verification option.”

Depending on your preferences, the second prompt might say:

- 1. Approve Sign-In Request** – “We’ve sent a notification to your mobile device. Please open the Microsoft Authenticator app to respond.”

Locate the notification on your mobile device and:

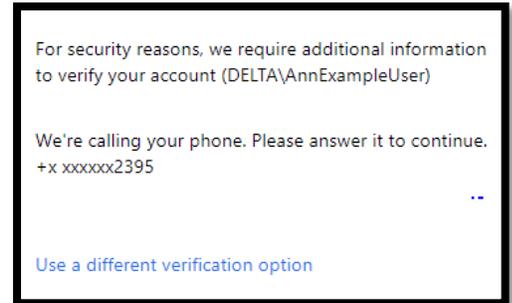


- Choose **Approve** only if you just initiated a sign-in.
- Choose **Deny** if you did not.

2. Approve Sign-In Request – “We’re calling your phone. Please answer it to continue.”

Answer the phone and:

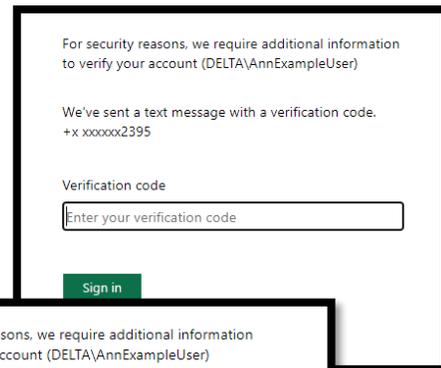
- Press # to verify if you just initiated a sign-in.
- Hang up if you did not.



3. Enter Code – “We’ve sent a text message with a verification code. +x XXXXXX1234.”

Locate the text message and

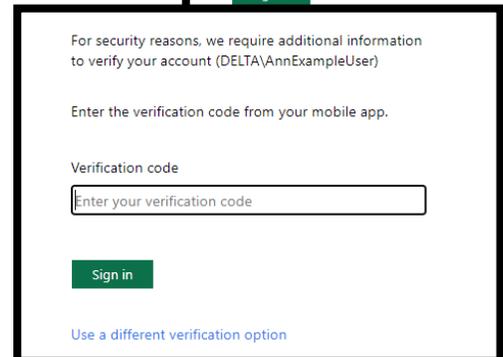
- Type the 6-digit code into the sign-on box.
- Don’t share this text message with anyone else.



4. Enter Code – “Please enter the code displayed on your authenticator app from your device”

Open the Authenticator app on your smart device or retrieve you hardware token and:

- Type the 6-digit code into the sign-on box.
- Don’t share this code with anyone else.



[\(Top\)](#)

I forgot my password. How do I get back into my account?

If you forgot your password or let it expire, please use the **Forgot Password** link at the bottom of the sign-on screen.

If you’re unable to regain access to your account using the **Forgot Password** link, you will need to contact the OIT Helpdesk by emailing help@delta.edu or calling 989.686.9575 to request help with recovering your account.

Recovering your account can be done in-person during normal business hours, using Photo ID.

This process **can** be done remotely but, depending on your situation, may take 1-2 business days to complete.

[\(Top\)](#)

What makes a good password?

- Longer is better, unless it's easily guessable.
- Using a phrase or sentence is better than just using a word.
 - "Eye-love-Lucy
- More types of characters is better.
 - The four character types are:
 - Upper Case Letter (A B C)
 - Lower Case Letter (x y z)
 - Number (1 2 3)
 - Symbol (@ # ^ *)
- Is completely different from passwords used for other electronic accounts.
- Is not a guessable variation of a password used for another electronic account.
 - Example:
 - If your password for Facebook is **1LoveLucy.FB**,
 - Using **1LoveLucy.DC** for Delta College would be a guessable variation if your Facebook password was exposed.
- An acceptable password for your Delta College electronic account must contain a minimum of 8 characters, 3 character types and not contain common passwords or variations.
- Examples of passwords meeting the first two criteria but would fail the "easily guessed" criteria are:
 - P@ssword
 - 8 characters, 3 character types, easily guessed.
 - Winter20!
 - 8 characters, 3 character types, easily guessed.
 - Delta1961.
 - 9 characters, 3 character types, easily guessed.

[\(Top\)](#)

Can I opt out of MFA?

As of November 1, 2020, multifactor authentication will be required for all electronic account holders. Please contact the OIT Helpdesk if you need assistance.

[\(Top\)](#)