

# Your security is our priority

You can feel safe knowing that every TIAA account has multi-factor authentication enabled to protect your online account from unauthorized access. Multi-factor authentication (MFA) utilizes not just one identification factor but multiple, making your login experience more secure. Read on to learn more about multi-factor authentication (MFA) and the steps TIAA has taken to implement MFA.

## What is multi-factor authentication?

Multi-factor authentication is a trusted and standard method for securely granting access to a website. The method works by verifying at least two or more identifiable factors from different categories: something you know, something you have and/or something you are. This method helps ensure only you can access your TIAA online account.

Some general examples of factors that can be used for multi-factor authentication include:



### Something you know

For example, your username and password, account ID or security questions



### Something you have

For example, a registered device, one-time passcode or RSA token



### Something you are

For example, biometric authentication (thumbprint, facial recognition, retinal scan)

**At TIAA, account security is one of our top priorities, therefore, we require multi-factor authentication to be met for all web and mobile logins. No action is needed to enable multi-factor authentication, however, TIAA also offers several different security options that you can opt-in to add even more layers of security.**

## Your security is our priority

---

To set up biometrics on the TIAA app, select to enable biometrics and proceed with storing your thumbprint or facial likeness to be used as an additional factor.

To set up a one-time passcode text on the browser-based TIAA website, login, select to view your 'Profile' and then select 'Security Preferences', where you can enable the setting for a one-time passcode to always be sent to your mobile phone.

### The power of your voice

Voice biometrics is also offered by TIAA as an easy but secure way to complete multi-factor authentication requirements for interactions with TIAA over the phone. Just enroll when calling in and use your voice to authenticate on all future calls.

