Duo Mobile - Using Verified Push with Office 365

Office 365 logins now require what's called a 'Verified Push' which differs from the standard Multi-Factor Authentication (MFA) Push. Duo Verified Push enhances the security of conventional MFA by requiring the user to enter a 3 digit code on your device to complete the login. You will no longer be offered the option to approve or deny a Duo push notification without entering the code provided when logging into Office 365 services.

This added layer of security helps individuals quickly identify and thwart potential phishing and other credential-stealing attacks. Duo Verified Push reduces the likelihood of accidental approval of malicious login attempts.

*Verified Push only works when combined with the Duo mobile app. SMS authentication is still supported for a limited time.

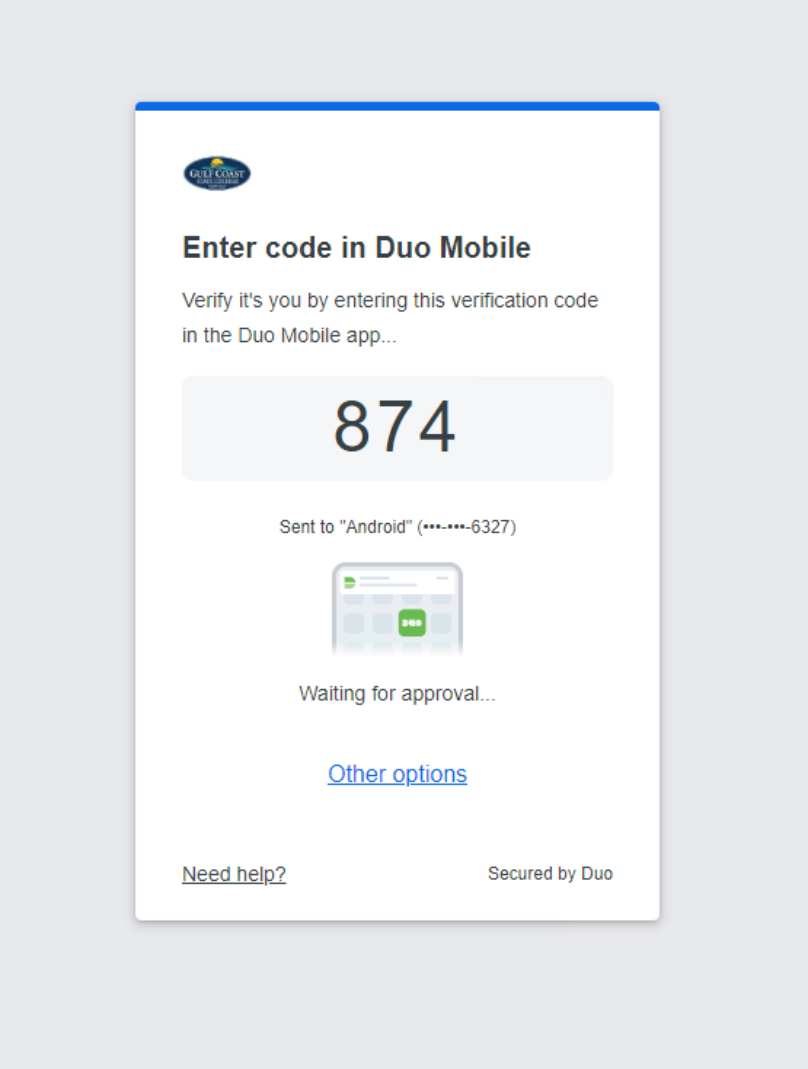
Verified Push Procedure

Duo App based MFA will prompt the individuals to accept or deny login with a push notification to their device. The login flow would generally look like this,

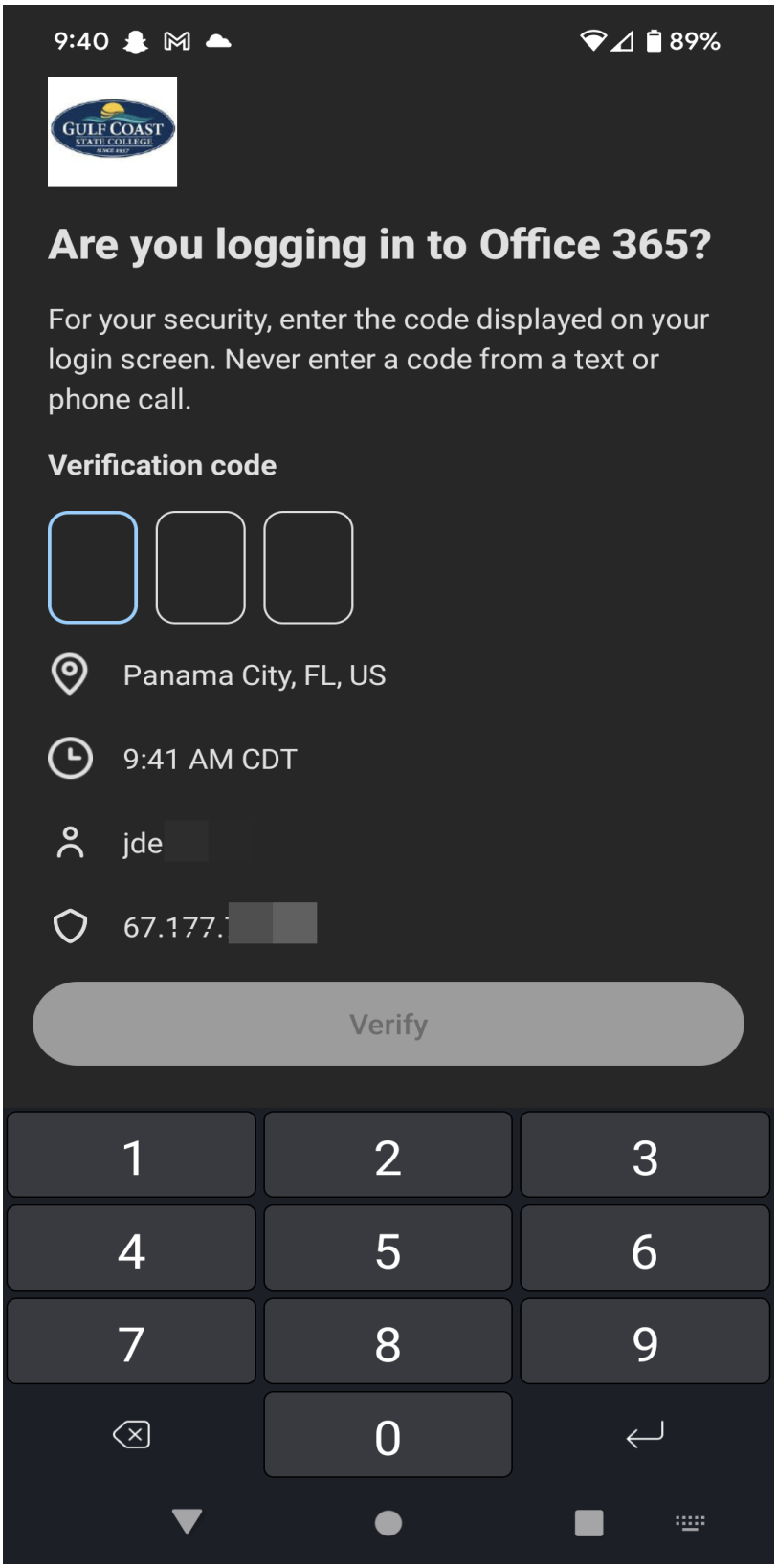
1. User logs into Office 365 with GCSC ID and password

2. The login process displays a screen similar to the one below with a random 3-digit code

At this time Duo is also sending a 'push' notification to the Duo app installed on the users registered device

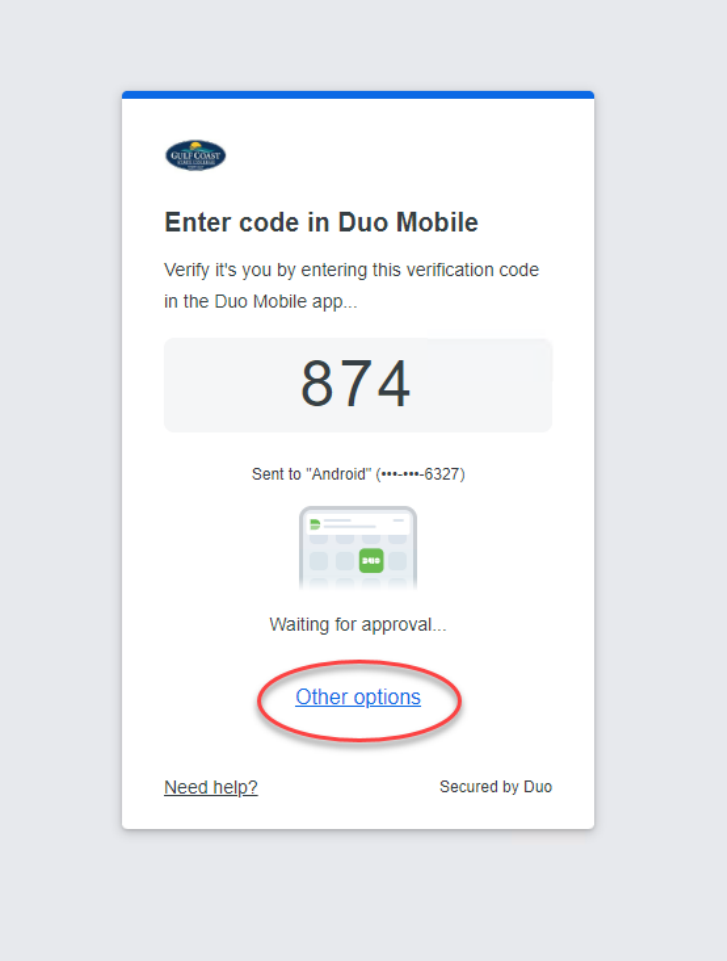


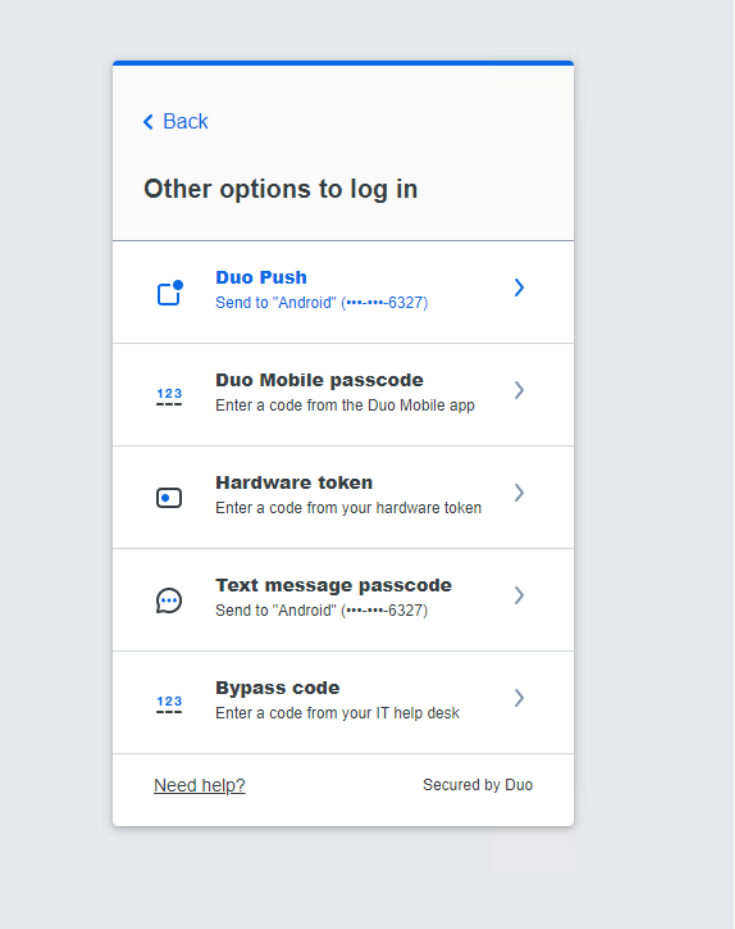
3. User should receive a notification on their phone requesting the code to approve the login. Individuals will enter the 3-digit code from the device's screen and tap Verify.


9:40
89%
Are you logging in to Office 365?
For your security, enter the code displayed on your login screen. Never enter a code from a text or phone call.
Verification code
Panama City, FL, US
9:41 AM CDT
jde
67.177.
Verify
1
2
3
4
5
6
7
8
9
0

That’s it!

- Alternately, there are ‘other options’ for MFA authentication such as text messages however these may be removed in the future.





Why will text / SMS be eventually phased out?

While a text message for second factor authentication provides an additional layer of security, it is important to note that SMS is prone to several vulnerabilities. For example, SMS lacks encryption which means that the information transmitted during the authentication process is not protected against potential interception. The rapid progress of technology has made it increasingly easier for attackers to intercept, manipulate, spoof, and impersonate text messages making it a less secure method and more susceptible to malicious activity. As a result, these vulnerabilities will eventually render SMS MFA obsolete, prompting the need for more secure alternatives.