STETSON UNIVERSITY
Information Technology

# Microsoft Two Factor Authentication with Number Matching

Microsoft Two-Factor Authentication with Number Matching utilizes Microsoft's Authenticator Application. If you do not have the application, please download it at

Apple App Store: https://apps.apple.com/us/app/microsoft-authenticator/id983156458

Google Play Store: https://play.google.com/store/apps/details?id=com.azure.authenticator

For directions to set up Microsoft Authenticator, please visit https://www.stetson.edu/administration/information-technology/multi-factor-authentication.php

The Authenticator app will now require users to type a number displayed on the screen to complete the authentication process.

A now common attack by criminals is attempting to trick individuals into approving an MFA phone push request. These are referred to as MFA fatigue attacks. The notification that appears on the victim's phone is a request to approve or deny a login request. The request was not generated by the victim's activity, but by the criminal attempting to login with the victim's username and password combination. The criminal will repeatedly send these requests to the victim's phone hoping that the victim will eventually approve one of these attempts. With both the password and MFA approval the criminal can access the victim's account.

To combat this security threat, Microsoft is enabling a feature called number matching. When a push notification is generated a two-digit code will appear for the login attempt. The user attempting to login will need to enter the two-digit code into their Microsoft Authenticator app.

To utilize the number matching feature when presented:

1. View the number on your device provided to you by Microsoft.
2. Enter the provided number into the Microsoft Authenticator application on your mobile device.