Faculty/Staff Multi-Factor Authentication

September 2018

Ray Drake
Director – Systems & Applications Support ITCS
Multi-Factor Authentication (MFA)

MFA is a security system that requires more than one method of authentication from independent categories of credentials to verify the user’s identity for a login.
Multi-Factor Authentication (MFA)

Security Initiative to protect university computing assets

Summer 2017 had >1000 users fall for phishing schemes. Resulting in account compromise, lockouts, account disabled, etc.

Phase I – Students
  • Pilot
  • Self-enrollment
  • Mandatory enrollment February, 2018

Phase II – Faculty/Staff
  • Fall Semester 2018
Multi-Factor Authentication (MFA)

Implementation -

Initial – Office 365 resources
  • OneDrive
  • Office Online
  • All Office 365 offerings (Yammer, OneNote, Delve, etc)
  • Faculty/Staff email

Required for “off campus” access

MFA is required for applications that don’t support Microsoft’s “Modern Authentication”. These will require an “app password”.

Future – additional ECU computing resources
Multi-Factor Authentication (MFA)

**Modern Authentication** – brings Active Directory Authentication Library (ADAL)-based sign-in to Office client applications across platforms.

A quick way to understand this: If you don’t use the purple login page for an application, you need to replace your ECU passphrase in the settings with an “app password”.

Examples needing an ‘app password’:
- Mobile **native** email client
- Outlook versions < v2016
# Multi-Factor Authentication (MFA)

<table>
<thead>
<tr>
<th>Method</th>
<th>How it works</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phone Call</strong></td>
<td>After signing in to pirate365.ecu.edu or piratemail.ecu.edu* using your PirateID and passphrase, Microsoft calls your phone. Click the pound (#) key to verify your identity.</td>
</tr>
<tr>
<td><strong>Mobile Phone Text</strong></td>
<td>After signing in to pirate365.ecu.edu or piratemail.ecu.edu* using your PirateID and passphrase, Microsoft texts a 6-digit code to your mobile phone. Enter the code to verify your identity. <em>Carrier standard text rates apply.</em></td>
</tr>
</tbody>
</table>
| **Mobile App**       | Download the **Microsoft Authenticator** app to your mobile device. After signing in to pirate365.ecu.edu or piratemail.ecu.edu* using your PirateID and passphrase, either:  
  - tap **verify** in the app or  
  - enter the one-time code to verify your identity. *(May use cell data)* |
| **App Password**     | System-generated password replaces your ECU passphrase in mobile email settings and other apps for which there is no sign-in screen.  
  Use one app password per device. |

* coming this fall

**NOTE:** users will be able to select to ‘trust’ a device and will not be required to MFA for 60-days on that device
Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account.

Step 1: How should we contact you?

Authentication phone

United States (+1)

Method

- Send me a code by text message
- Call me

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account.

Step 1: How should we contact you?

Mobile app

How do you want to use the mobile app?

- Receive notifications for verification
- Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

Set up Mobile app has been configured.
Multi-Factor Authentication (MFA)