Duo Two-Factor Authentication

Bobby Jones
Lead Software Support Analyst
System Enterprise Application Support
bcssupport@tamus.edu
979.458.6450
http://it.tamus.edu/sso/
Why two-factor authentication?

- Result of a successful phishing attempt
  - Several employees had fake tax returns filed in their name
- Required of administrative roles that access potentially sensitive data
  - Employees, Managers and Approvers aren’t required
- Even if UIN credentials are compromised the account is still secured
Misconceptions

- Cell phone is required
  - Most administrators prefer their office phone

- Have to use Duo for every log in
  - Use the ‘Remember this device’ feature

- Cell phone users must install the app
  - Pass codes and phone calls can also be used

- Can only use one device
  - Multiple devices can be enrolled
Administrative Features

- SSO Admins can add/delete devices
  - Only if they have the ‘password reset’ permission
- SSO Admins can require an employee to use two-factor authentication
- SSO and Duo are two separate accounts
  - Only System Enterprise Application Support can unlock a Duo account
Final Thoughts

1. Cell phone isn’t required nor is the Duo Mobile app
2. SSO Admins can add/delete devices
3. Contact BCSSupport@tamus.edu to unlock an employee’s Duo account
We’re here for you!

HUMAN RESOURCES
LIAISON NETWORK
FY2016

HR Liaison Network