Multi-factor Authentication (MFA) Update

Jeff Hollingsworth
Interim CIO

Why Multi-factor Authentication

- Prevents common security problems
  - Password alone is not enough to gain access
- Recent incidents that MFA could have prevented
  - University of Iowa Grade Changing (Mar 2015- Dec 2016)
  - Compromise of DNC Email (Summer/Fall 2016)
  - Compromise of Consulting firm Deloitte's Email (Fall 2017)
  - UMD Grade Changing (two incidents Spring 2017)

One Compromised Email Address Causes Reputational Damage

- Can expose sensitive information
  - FERPA data
  - Employee Information (references, etc.)
- Can block email for thousands of UMD users
  - Email address used to send large amounts of Spam
  - Results in the entire university being blocked from some email providers

DUO MFA Solution

- Supports Multiple Modes of Authentication
  - Smart phone apps (IOS & Android)
  - Hardware tokens
  - Call to a registered number
  - One time codes
- Used by
  - Many Big 10 Schools
  - Etsy, Facebook, Yelp, …

Authority for MFA Requirement

- University Policy X-1.00(A) which states "Those using University IT resources, whether at the University or elsewhere, are responsible for complying with security standards set forth by the Vice President and Chief Information Officer (VP/CIO)"
- As CIO, I set a security standard that MFA must be used for CAS logins by specific dates.

Timeline for Mandatory Use of MFA

- Data Warehouse Access (May 2015)
- Kauli Financial System Access (May 2015)
- Division of IT Employees (March 2017)
- Faculty/Graduate Asst./Deans/Directors/VPs (Dec 2017)
- Emeritus Professors (Feb 2018)
- Rest of Staff (March 2018)
- All Students (TBD – likely Fall 2018)

Report of Monday Deadline

- 74% of faculty/GAs have enrolled by 11/28/17
- Call center handled YY calls on MFA on Monday
- ZZ users logged in via MFA on Monday

Questions?