MULTIFACTOR AUTHENTICATION WITH DUO SECURITY

University of Idaho

ITS SECURITY

ITS-Security@uidaho.edu

University of Idaho
Information Technology Services
YOUR FEEDBACK IS IMPORTANT!

- Contact us directly or use https://www.uidaho.edu/mfa
- New date for Employees: January 17, 2018 to allow everyone to enroll on their own timeline and get any assistance they need
- Hardware tokens will be available in December and will be available at no cost to all (Duo mobile still preferred)

PASSWORDS ARE NOT ENOUGH

- 300% increase from 2016 to 2017 in user accounts attacked (Microsoft Security Intelligence Report, Volume 22)
- 81% of breaches from stolen or weak passwords (Verizon Data Breach Investigations Report, 2017)
- Breaches are very expensive, even with insurance
Local Threat

PASSWORDS ARE NOT ENOUGH

• 165 UI accounts known compromised in last two years
• 29 users with Direct Deposit changed, a few checks lost
• Not just paychecks and identity theft, attackers are after:
  • YOUR PERSONAL INFORMATION
  • Financial Aid disbursements
  • Intellectual Property, including Library and Research publications
  • Platform to attack others (phishing, lateral movement)
• Past phishing exercises show a constant 15-19% click rate for any group of U of I users, even after training

Compliance

REQUIRED IN SELECT AREAS

• FISMA/NIST requirements are being tied to research ($$$)
  • SP800-171 Control of Unclassified Information
• Governor’s Executive Order on Cybersecurity
  • Critical Security Controls
• Payment Card Industry (PCI-DSS)
• HIPAA best practice (employee benefits)
Strength?

**PASSWORDS**

- Longer passwords are better for brute force attacks
- Once a password is stolen, it doesn’t matter if it is long or short, simple or complex
- Password leaks are frequent (Dropbox, Yahoo, etc.)

**MULTIFACTOR AUTHENTICATION (MFA)**

- **Something You Know**
  - A password
  - Answer to a Security Question
- **Something You Have**
  - A trusted device (i.e. Smart Phone, Smart Card, Hardware Token)
- **Something You Are (not used in our deployment)**
  - A Fingerprint
- Alone, each method can be forged, but two or more together are much stronger
DUO SECURITY

• Duo integrates MFA with many different systems
• 5 million users | 8000+ customers | 6 Million authentications per day
• Duo has been chosen by more than 150 universities
  ▪ Arizona State, Portland State, Colorado State, Utah schools, Indiana University, University of Washington and many more
• Duo has been chosen by many well-known corporations
  ▪ Etsy, Facebook, Toyota, Zillow and many more

SYSTEMS THAT WILL REQUIRE MFA

• Anyplace with SSO
  ▪ Vandalweb, Bblearn, etc.
• Office 365 applications
• VPN
• Help.uidaho.edu
• (more in the future)
• NOT desktop logon
PLATEFORMS SUPPORTED

• NOT a Microsoft-only solution
• All mail clients that work today can be supported (Enable Legacy email)
  • Mail and Calendar on OS X
  • Thunderbird and similar IMAP clients
  • Android Mail and Calendar
  • iOS 10 and before Mail and Calendar

HARD TOKEN
OTHER FAQS

- Duo Mobile gives U of I no control of personal devices – only visibility into security posture (out of date, etc.)
- Checking “Remember me” will remember the browser and computer for 14 days, even in the classroom
- Internet connection is not needed for Duo Mobile – it can also act as a software token – but very little data used
- More FAQs at [https://www.uidaho.edu/mfa](https://www.uidaho.edu/mfa)