Two-Factor Authentication at the U.

Presented June 20, 2016
Kinesiology
Agenda

- What is two-factor authentication?
- Why is it important?
- Where is it used?
- What are the benefits?
- How does it work?
- Summary
Two-factor authentication provides a second layer of security to any type of login, requiring extra information or a physical device to log in, in addition to your password.
What is Used For Authentication?

- Something you know (e.g., PIN, password)
- Something you have (e.g., a hardware or software token, a notification)
- Something you are (e.g., fingerprint, voice)
- Someplace you are (e.g. physical or network)
- Someone who knows you
Why is this important?

- Provides an additional layer of security.
- Protects your information even if your credentials are stolen.
- Makes sites that use 2FA less attractive to the bad actors.
Where is it currently used?

2FA is used on the following systems:

- HR Management
- Faculty Business
- Financials & Physical Resources System
- Manager Desktop
- Report Library
- Student Administration

- M-Reports
- Report Library
- U-M Data Warehouse (only when accessed with BusinessObjects)
- Time Approval
Where is it currently used?

2FA is used on the following systems:

- DART (Donor Alumni Relationship Tool)
- MCommunity Sponsor System
- Flux Computing Cluster
- MiChart Electronic Prescribing for Controlled Substances (EPCS)
<table>
<thead>
<tr>
<th>Benefits</th>
<th>Improved data security</th>
<th>Increased productivity</th>
<th>Improved strategic alignment &amp; capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Faster and easier integration</td>
<td>● Variety of different authentication methods to fit different use cases</td>
<td>● Self-service capabilities</td>
<td>● Cloud solution</td>
</tr>
<tr>
<td>● Enterprise licensing</td>
<td></td>
<td></td>
<td>● Common and scalable solution</td>
</tr>
<tr>
<td>● Increased user adoption</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How does it work?

Enter username and password

Verify identity

Securely logged in
New 2FA Vendor
## Options

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Push</th>
<th>Passcodes</th>
<th>SMS Passcodes</th>
<th>Phone Callback</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Duo sends a login request to your phone. Just tap Approve to authenticate.</td>
<td>Generate a passcode when needed using the Duo app.</td>
<td>Receive a batch of passcodes via text message.</td>
<td>Duo calls your phone. Just press any key to authenticate.</td>
</tr>
<tr>
<td><strong>Platforms</strong></td>
<td>iOS</td>
<td>All Push platforms, plus Palm, Windows Mobile</td>
<td>All phones with SMS</td>
<td>All phones</td>
</tr>
<tr>
<td>Usable without WiFi or Cellular Service</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

*Hardware tokens are available if you have a specific business need*
High Level Implementation Roadmap

May 16
ITS Pilot of current MToken/Weblogin users

June
UMHS - Also enrolling VPN users

July
Enrollment of current MToken/Weblogin users: AA, Dbn, Flint

July 20
Transition Unit Servers and Applications to Duo 2FA; units to initiate contact with ITS and refer to documentation

Aug-Dec
Cutover to Duo
Expand 2FA across campus

Opt-in enabled for Wolverine Access and M+Google
Faculty may begin using Duo 2FA for sensitive information
Retire RSA vendor Dec 2016
Demo

The Cosign login page is changing 7/20/16

Link to enroll

https://password.it.umich.edu/pwm/private/

More information

http://its.umich.edu/two-factor-authentication

http://documentation.its.umich.edu/2fa/enroll-smartphone-or-tablet-duo
Questions?

2Factor at The U
http://www.itcs.umich.edu/identity/2factor/

2fa.project.contact@umich.edu

Say Yes to Multifactor Authentication
http://safecomputing.umich.edu/content/newsletter/#mfauthtip
Additional Available Presentations

- General Security
- Personally Owned Devices
- Phishing
- Sensitive Data Scanning
Remember, it’s good for you, and good for the U.