2-Factor Authentication for Smith

Ben Marsden, Information Security Director
InfoSecurity@smith.edu
April 2017
What is 2-Factor Authentication?

- **2FA** adds a small but very effective security step to your Smith Single Sign On login to help protect your account even if your password gets stolen.

- We are using **DUO** for our 2FA service.

- **Duo** uses a **second device** to verify your identity.

- Makes it very difficult for an imposter to use your Smith account to access our services and your information.
Why do we need it?

- **Passwords alone are weak security!**

- This extra step will greatly enhance your account’s security, and help protect:
  - your information in Banner, including your SSN and other personal information
  - your email communications
  - access to licensed resources and restricted services
  - access to course work, research data, and intellectual property you own or create

- And will help you avoid the trouble of cleanup, time loss, and personal harm that results when your account gets used by a cyber criminal!
How does it change what I do now?

- Duo adds a quick identity verification step to your Smith login process.
How does it work? (the process)

1. Launch a browser
2. go to a Smith service that uses SSO
3. login with your Smith username and password
4. choose a Duo device and method
5. approve the login request

YOU ARE SAFELY LOGGED IN!
How does it work? (the security)
## Device options for Duo verification

<table>
<thead>
<tr>
<th>Supported Devices</th>
<th>Duo Mobile App</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Push Notification</td>
<td>Passcode</td>
<td>SMS (Text)</td>
<td>Phone Call</td>
</tr>
<tr>
<td><strong>Smart Phone</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Wifi Enabled Tablet</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Cell Phone</strong></td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Landline</strong></td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Hardware Token</strong></td>
<td></td>
<td></td>
<td></td>
<td>Plug the token into your computer's USB port and touch to verify your login.</td>
</tr>
</tbody>
</table>
How do I get started?

- First, **sign up** for Duo by following “Step 1” in the link below
  - Duo sign up requests are automatically processed around 9 am each morning

- The next day (if you signed up after about 10 am) login to the Smith portal and follow the popup instructions to **register your devices**.

- Go to our Duo web site here and follow the steps to get started:

  [https://www.smith.edu/tara/security/duo.html](https://www.smith.edu/tara/security/duo.html)
Quick hints and Best Practices:

- **Be sure to register at least two devices in Duo**
  - We recommend your mobile phone and your office phone

- Do **not** set Duo to autopush to your smart phone.

- Only select “Remember me for 30 days” on your primary computer.

- Get a list of one-time codes and store them in a safe place.

- If you’re self-enrolling, don’t sign up on a Friday!

**And also:**

- Update your Emergency contact information in Banner.
- Set your smart phone to allow Duo to show alerts.
Questions (and sign up)

[https://www.smith.edu/tara/security/duo.html](https://www.smith.edu/tara/security/duo.html)

If you are registering a smart device, download the Duo Security app now!