THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

2023 FAST Conference - Phishing

Jeremy Shelley, CISO

What is phishing?

- Phishing consists of unauthorized individuals sending emails or other messages purporting to be from reputable companies or individuals.
- In the past few weeks OIT has seen phishing emails pretending to be:
  - Dr. Karr
  - Various UAH faculty
  - A faculty evaluation document
  - Kelloggs Food Group
  - Bank of America
  - Voice Message from a phone number claiming to be from Microsoft
  - “Dr. Richard”

What Is OIT Doing about Phishing?

- The UAH Office of Information Technology has several initiatives in place to prevent, detect, and even stop phishing attacks
- However, it is not enough; it takes the entire UAH user community must remain vigilant to help keep UAH safe
- For the UAH user community, here are the primary tools we offer.

SIMULATED PHISHING CAMPAIGNS

2-FACTOR AUTHENTICATION

Phishing Example #1

Paul Dandurand shared an item

Paul Dandurand (pdandurand@bozrah.org) has shared the following item:

Dr. Charles L. Karr has shared a file with you for review.

2022-2023 Faculty Evaluation .Docx.pdf

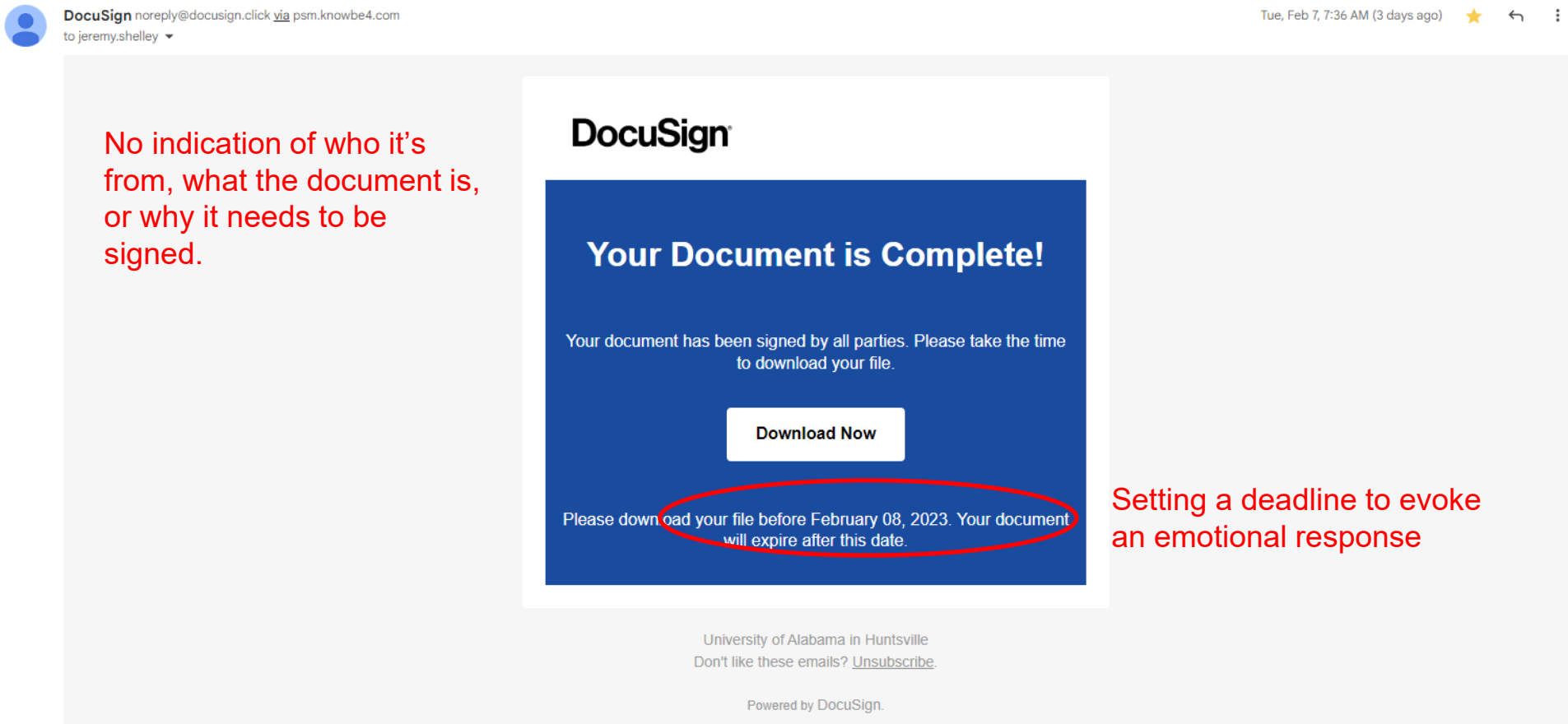
Paul Dandurand is outside your organization.

If you don't want to receive files from this person, block the sender from Drive

Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
You have received this email because pdandurand@bozrah.org shared a file or folder located in Google Drive with you.

Google Workspace

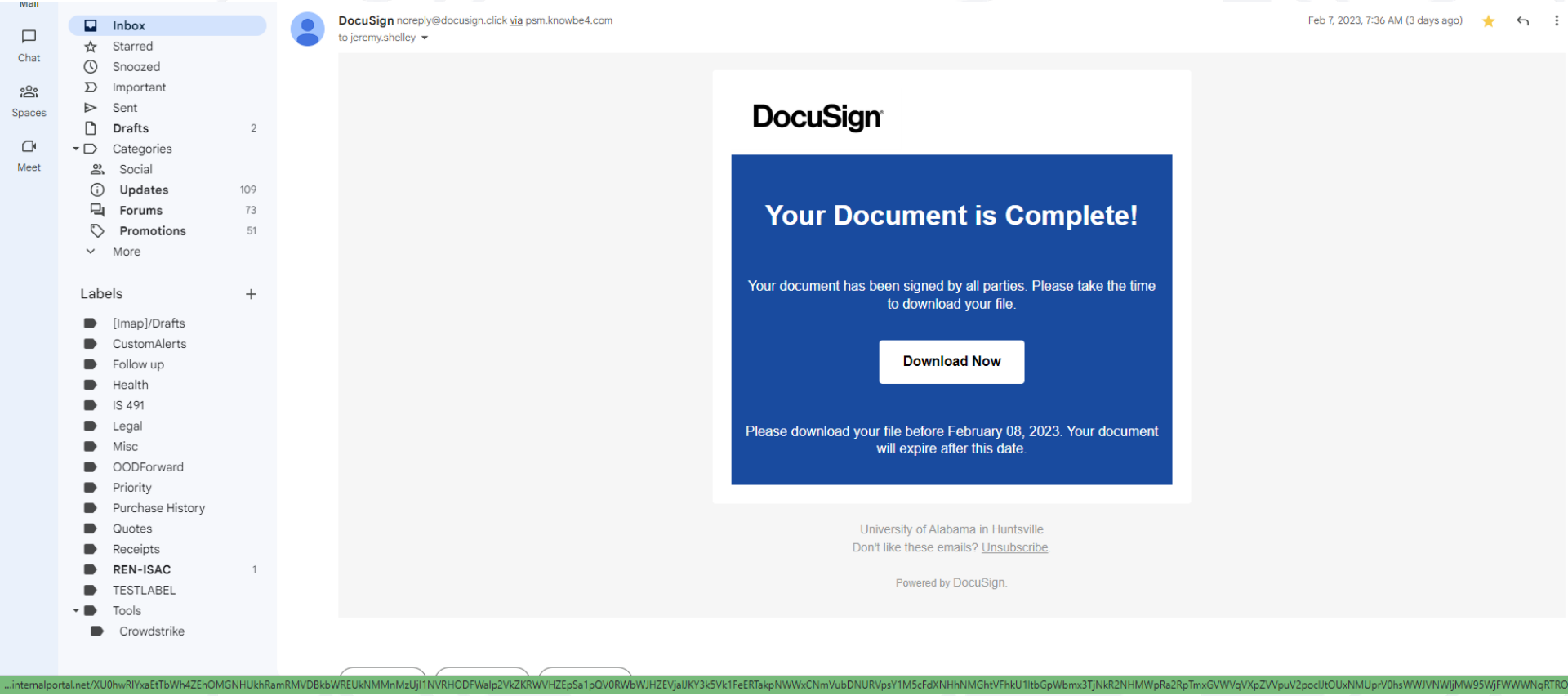
Phishing Example #2



No indication of who it's from, what the document is, or why it needs to be signed.

Setting a deadline to evoke an emotional response

Phishing Example #2



When hovering over the “Download Now” button or “Unsubscribe”, the link goes to exchange.internalportal.net, not Docusign

What to look for in an email?

- Look for the “[EXTERNAL]” label on emails
- Want you to click a link to
  - Make a payment
  - Claim a prize/refund
  - Review an invoice
  - Update your antivirus software
  - Update your account information
  - Download a file
- Warning signs
  - Generic or unfamiliar greeting
  - Message makes threats or tries to invoke a sense of urgency
  - Message contains grammar or spelling errors
  - Inconsistent email addresses, links, domain names
  - Message claims to be from someone at UAH but comes from a non-UAH email address
  - Artificial and short deadline

What do I do if I receive a phishing email?

- Do not click on a link or open an attachment.
- Click on the 3 dots in the top-right corner of the email and click “Report phishing” or “Report spam”.
  - This notifies both Google and the UAH team.

- If you clicked on a link or responded to an email you discover is spam
  - Immediately go to https://reset.uah.edu and change your UAH password
  - Contact the Help Desk
    - helpdesk@uah.edu
    - 256-824-3333

Thank You for Your Time

- Remember that we all have a cybersecurity role here at UAH.
- If you see something, say something.
- Remember, #StayVigilantStaySafe

IT-SIRT@uah.edu

256-824-3333