ALTA
American Land Title Association

ALTA inSIGHTS

REAL TIME | ON-DEMAND

Best Practices to Identifying Phishing Email

June 12, 2024

Today's ALTA Insights Featured Sponsor

Speakers

KLOUD9

Trent Milliron,
CEO

Dickon Newman,
ISSO *(Information System Security Officer)*

Poll Question

What is phishing?

Phishing is a type of email attack.
Typical controls are no longer effective. The least effort / highest payoff method is through the employee, even CEO's.

It is a form of Social Engineering. What is Social Engineering?

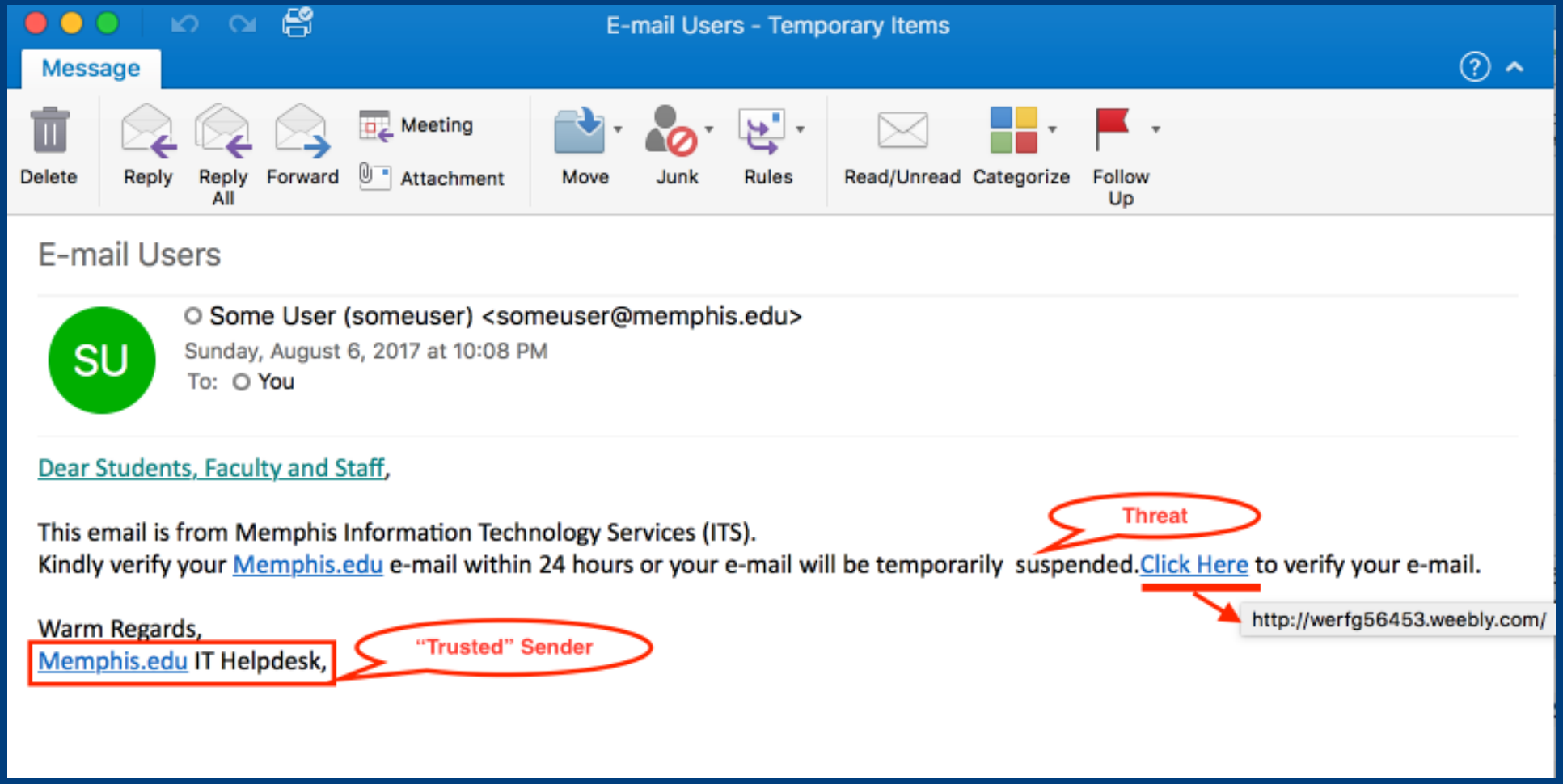
Call to action – Click, call, purchase, open, etc.

The attacker is trying to infect, or otherwise garner information that can be used in a larger attack.

SLAM Method

- Sender
  - Check the sender – review email/domain accuracy
- Links
  - Mouse-over or hover over links, is the URL correct?
- Attachments
  - Trusted source? PDF's are common malware attempts
  - Invoice emails, package tracking, or payment confirmations
- Message
  - Review content. Normal? Typos? Strange cadence?

Examples of phishing?



Examples of phishing?

From: **GlobalPay <VT@globalpay.com>** Hide
Subject: Restore your account
Date: February 7, 2014 3:47:02 AM MST
To: David

1 Attachment, 7 KB **Save** **Quick Look**

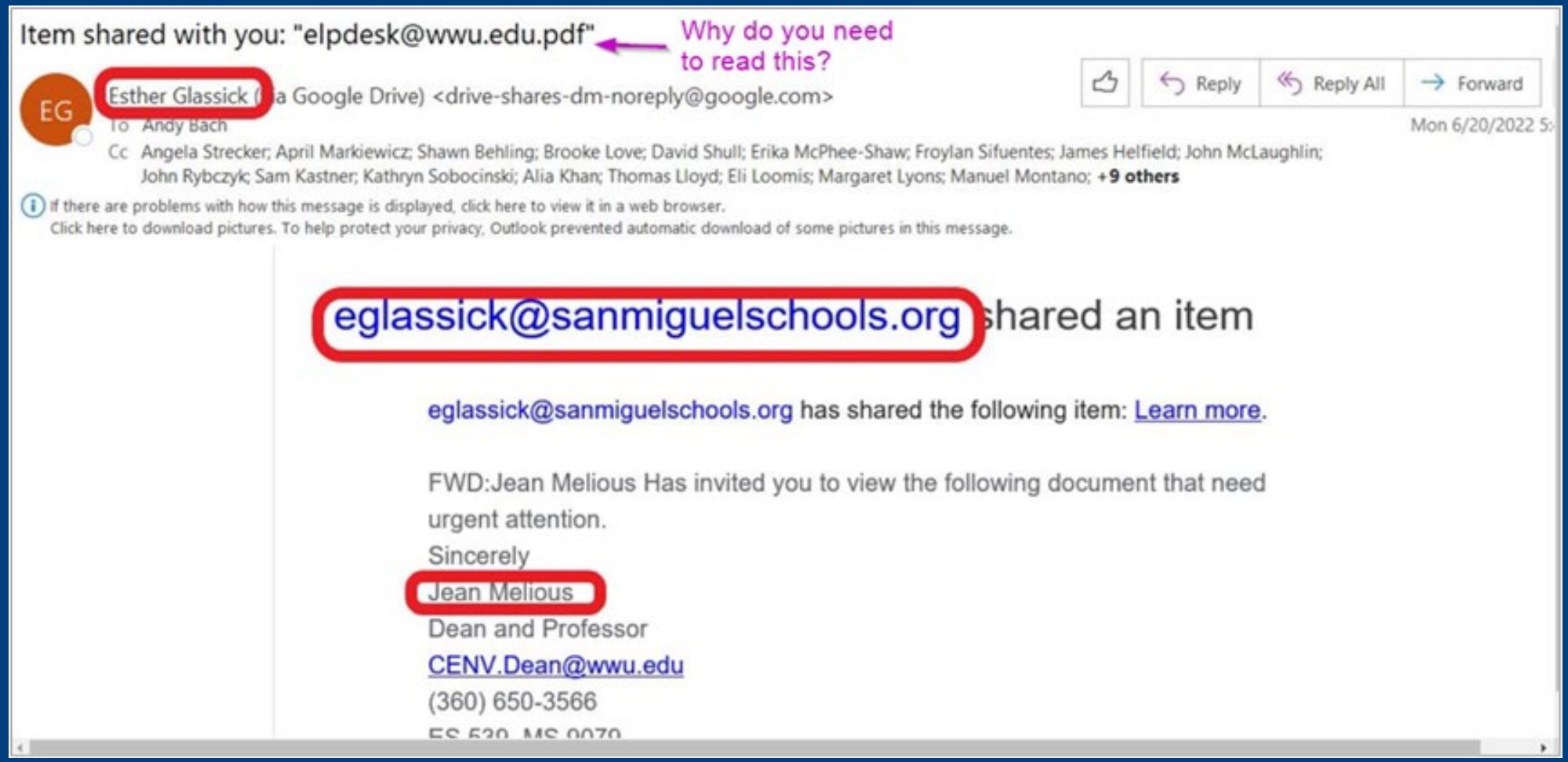
Dear customer,

We regret to inform you that your account has been restricted.
To continue using our services plese download the file attached to this e-mail and update your login information.

© GlobalPaymentsInc

update2816.html (7 KB)

Examples of phishing?



What to do?

If you have an email, you think is phishing:

- Have your MSP or internal IT department review the email
- Links may be bogus…go to the original vendor/customers website, and follow links on their site
- Phone numbers may be bogus…call the company directly on a known good number
- Do not click, open, or otherwise engage with the email and the call to action.
- If nothing else, at least delete the email!

What to do?

- If you do accidentally click a nefarious link:
  - Contact your MSP or internal IT department immediately and tell them what happened
  - Make sure your anti-virus or end-point-protection is up to date and scanning
  - Perform a malware scan with persistence and foothold checks
  - Depending on the extent of a potential compromise, consider triggering your Incident Response Plans
  - Consider resetting user passwords

Poll Question

Training employees

If employees are the weakest link, recurring training and refresher training is the only solution.

- Perform annual security awareness training at least annually and upon hire. Perform refresher training.
- Have robust policies in place (company handbook). As well as Incident Response Plans (that have been tested and disseminated)
- If you are a client of Kloud9, you receive FREE security training for your staff with continuous threat training.

Other Best Practices

Title Industry – FTC Safeguards

About 4 pages, broken into two sizes for small vs. large companies

Under 5000 Consumers

- Documented security plan & policies
- Designate a security officer
- Inspect and test
- MFA
- Encryption at rest & in transit

Over 5000 Consumers

- *Everything on the left plus…*
- Risk Assessment
- Continuous monitoring *OR* PEN tests & AVS scans
- Written and tested IRP
- Report annually to the Board of Directors

Rule change Oct 2023 – Incident reporting to FTC.

Q&A

ALTA
American Land Title Association

Contact Us

American Land Title Association
Protect your property rights

Speakers

- Trent Million | tmilliron@kloud9it.com
- Dickon Newman | dnewman@kloud9it.com

Company

- Kloud9 IT
- MSP and security services
- FTC Safeguards expertise and implementation, including policies
- www.kloud9it.com
- 844-556-8394