

# ALTA

# inSIGHTS

REAL TIME | ON-DEMAND



## Best Practices to Identifying Phishing Email

June 12, 2024

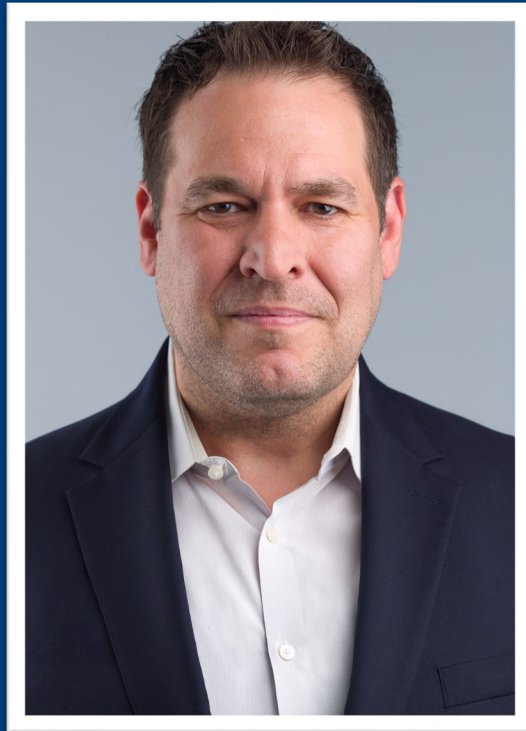
Today's  
ALTA Insights  
Featured  
Sponsor



**Closinglock**

# Speakers

# KLOUD<sup>9</sup>



**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.

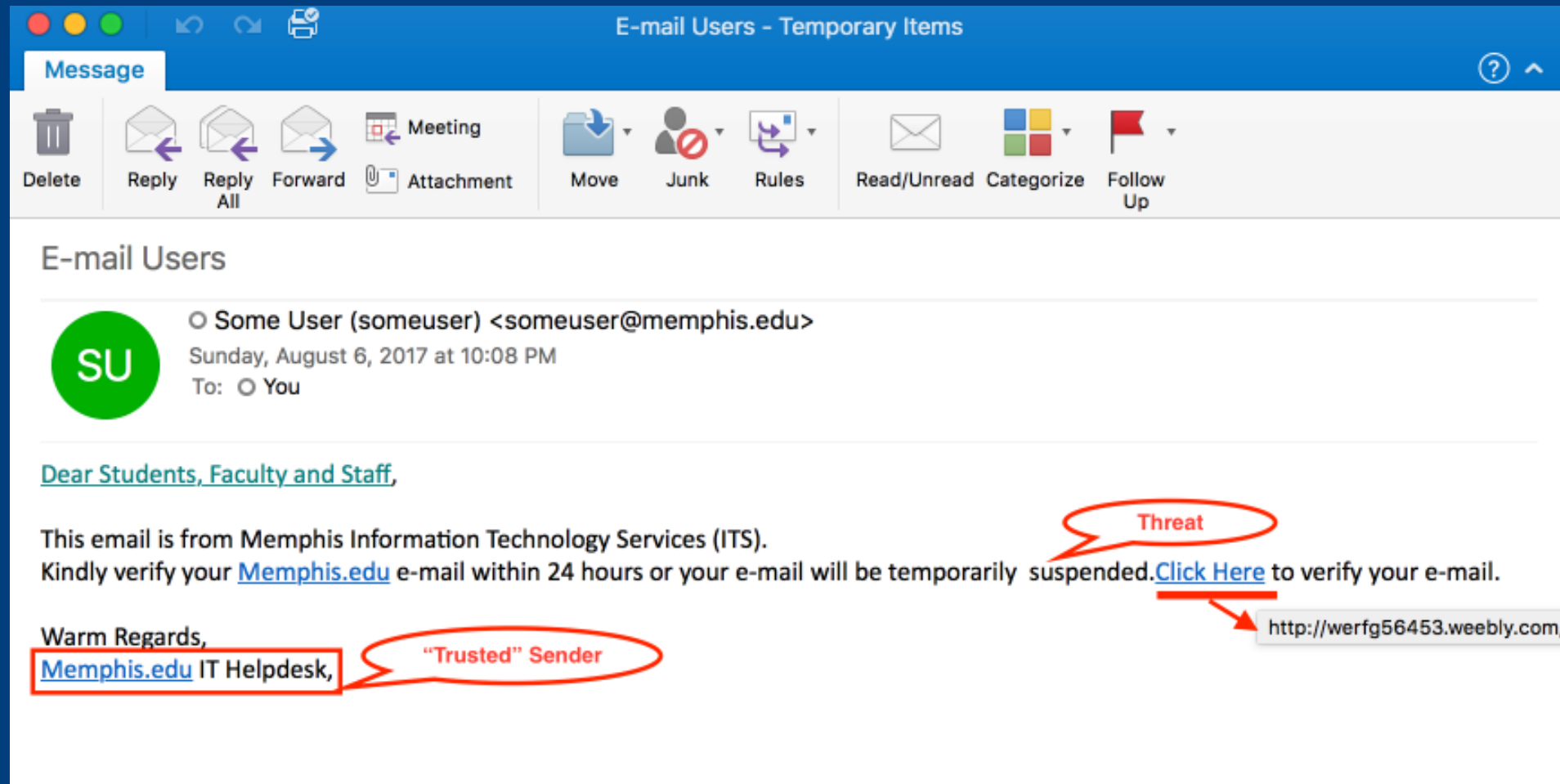


# SLAM Method

- **S**ender
  - Check the sender – review email/domain accuracy
- **L**inks
  - Mouse-over or hover over links, is the URL correct?
- **A**ttachments
  - Trusted source? PDF's are common malware attempts
  - Invoice emails, package tracking, or payment confirmations
- **M**essage
  - Review content. Normal? Typos? Strange cadence?




# Examples of phishing?



**Message**

Delete Reply Reply All Forward Attachment Meeting Move Junk Rules Read/Unread Categorize Follow Up

**E-mail Users**

 **Some User (someuser) <someuser@memphis.edu>**  
Sunday, August 6, 2017 at 10:08 PM  
To: You

[Dear Students, Faculty and Staff,](#)

This email is from Memphis Information Technology Services (ITS).  
Kindly verify your [Memphis.edu](#) e-mail within 24 hours or your e-mail will be temporarily suspended. [Click Here](#) to verify your e-mail.

Warm Regards,  
[Memphis.edu IT Helpdesk,](#) **"Trusted" Sender**


**Threat** (circled in red) points to the text: "or your e-mail will be temporarily suspended."

**Threat** (circled in red) points to the link: "[Click Here](#)"

<http://werfg56453.weebly.com/>



# 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 please download the file attached to this e-mail and update your login information.

© GlobalPaymentsInc

  
[update2816.html \(7 KB\)](#)



# Examples of phishing?

Item shared with you: "elpdesk@wwu.edu.pdf" ← Why do you need to read this?

EG Esther Glassick (via Google Drive) <drive-shares-dm-noreply@google.com>

To: Andy Bach

Cc: Angela Strecker; April Markiewicz; Shawn Behling; Brooke Love; David Shull; Erika McPhee-Shaw; Froylan Sifuentes; James Helfield; John McLaughlin; John Rybczyk; Sam Kastner; Kathryn Sobocinski; Alia Khan; Thomas Lloyd; Eli Loomis; Margaret Lyons; Manuel Montano; +9 others

Mon 6/20/2022 5:...

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.  
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

**eglassick@sanmiguelsschools.org** shared an item

eglassick@sanmiguelsschools.org has shared the following item: [Learn more.](#)

FWD:Jean Melious Has invited you to view the following document that need urgent attention.

Sincerely  
**Jean Melious**  
Dean and Professor  
[CENV.Dean@wwu.edu](mailto:CENV.Dean@wwu.edu)  
(360) 650-3566  
ES 520 MS 0070



# 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



# Contact Us

## Speakers

- Trent Million | [tmilliron@kloud9it.com](mailto:tmilliron@kloud9it.com)
- Dickon Newman | [dnewman@kloud9it.com](mailto:dnewman@kloud9it.com)

## Company

- Kloud9 IT
- MSP and security services
- FTC Safeguards expertise and implementation, including policies
- [www.kloud9it.com](http://www.kloud9it.com)
- 844-556-8394

