June 2026 Phishing Results

OIT's June phishing simulation email was titled, *Insurance Document Available for Your Attention*. The scenario included a link requesting the recipient to "VIEW FILE". The email requested the user to review the document which was allegedly sent from Adobe cloud.

Clues to Spot in this Scenario:

Issue: Legitimate sharing services are also used by attackers for malicious activity
Adobe Docusign, and other cloud sharing services, provide users a convenient and secure way to send and receive important documents from a trusted brand. Attackers use reputable services to make phishing emails look legitimate, then redirect users to fake websites that capture usernames and passwords.

What to do:
Never rely on an email alone. Always verify signing requests through a trusted, independent channel. Do **not** use links or contact information provided in the email. Instead, contact the sender using a known phone number or verified contact method. When possible, establish verification procedures with third parties in advance. Before taking action, confirm the **who, what, and when** of the request:

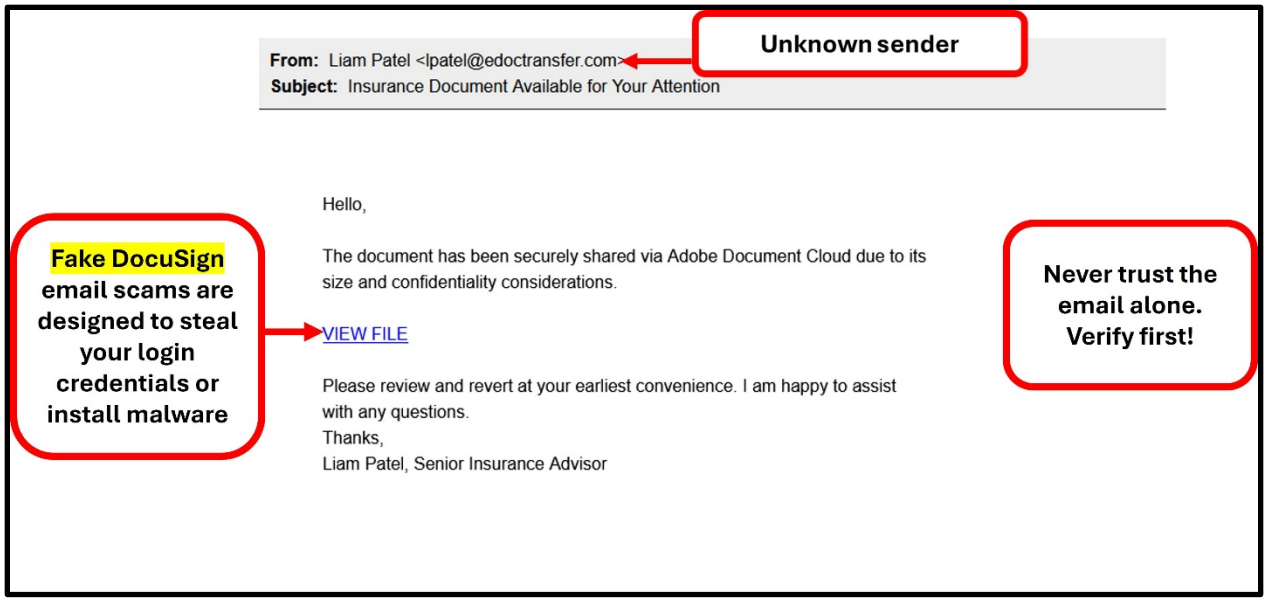
- **Who** will be sending the document?
- **What** is the sending email address and from what domain?
- **When** will the email be sent?

Issue: Unknown Sender
The sending email address was *Liam Patel <lpael@edoctransfer.com*. The email domain is unknown and should not be trusted.

What to do:
The simple rule is if the sender is unknown report the email as suspicious. Do not click on the link to find more information.

Always report emails that are unexpected and from an unknown sender, especially one that lacks specific content.

View the full scenario:



Good News

625 employees reported the phishing scenario. Great job MC!

Opportunities for Improvement

79 employees clicked the link

If you suspect an email may be a phishing attempt, let IT Security analyze the email for you by Reporting the email using the report phishing button.