February 2025 Phishing Scenario Results

As part of our Security Awareness Education Program, OIT sent a simulated phishing scenario titled, *FYI: Find Attached Doc 02/12/2025*. The email resembled Microsoft OneDrive's cloud storage document sharing application and provided a link to "View" a document.

Phishing emails are most successful when recognizable brands are used. These simple brand impersonation tactics easily trick you into trusting the sender and content. Even legitimate OneDrive accounts may be used in phishing emails! Remember to pause and review the sender, subject, and content.

This scenario gave multiple suspicious triggers:

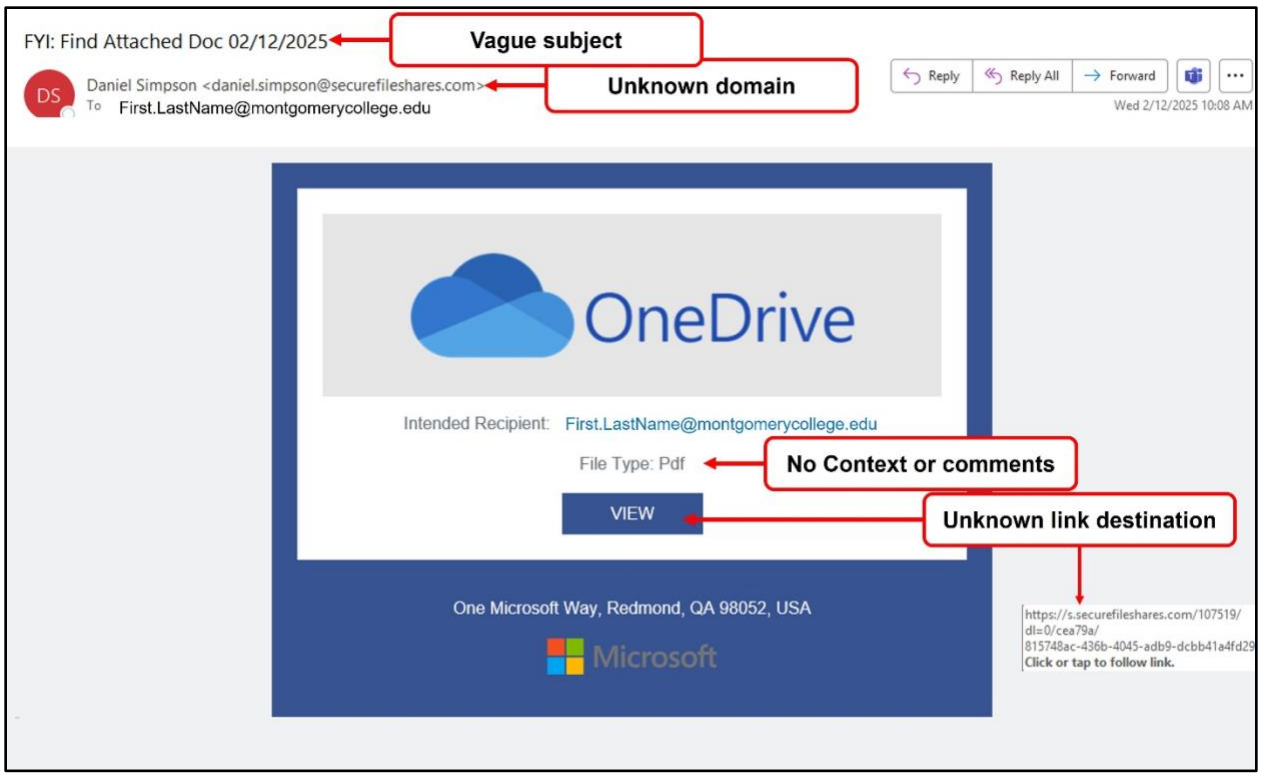
- unknown sending domain [@securefileshares.com]
- unknown sender [Daniel Simpson]
- vague subject [FYI: Find Attached Doc 02/12/2025]

Best practice is to **NOT** click a link when you were not expecting a shared document, especially from an unknown sender. If you *do* know the sender, take the time to review the sending domain and the reason they may be sharing.

Good news: 1129 employees reported the phishing scenario to the Phishtrap. **Nice work MC!**

Opportunities for Improvement: 167 employees clicked the link within the training email. Ouch! We can do better!

The attacker's goal is to capture your login credentials! In a real-world phishing attack clicking the link may have prompted you to give up your login credentials. **View the red flags in the February phishing scenario** to learn about this type of attack and ways to spot a suspicious email.



What should you do if you suspect an email may be a phishing attempt?

Let IT Security analyze the email for you – **REPORT** the email! The report phishing button within your email application allows you to quickly report suspicious emails to IT Security.