February 2024 Phishing Scenario Results

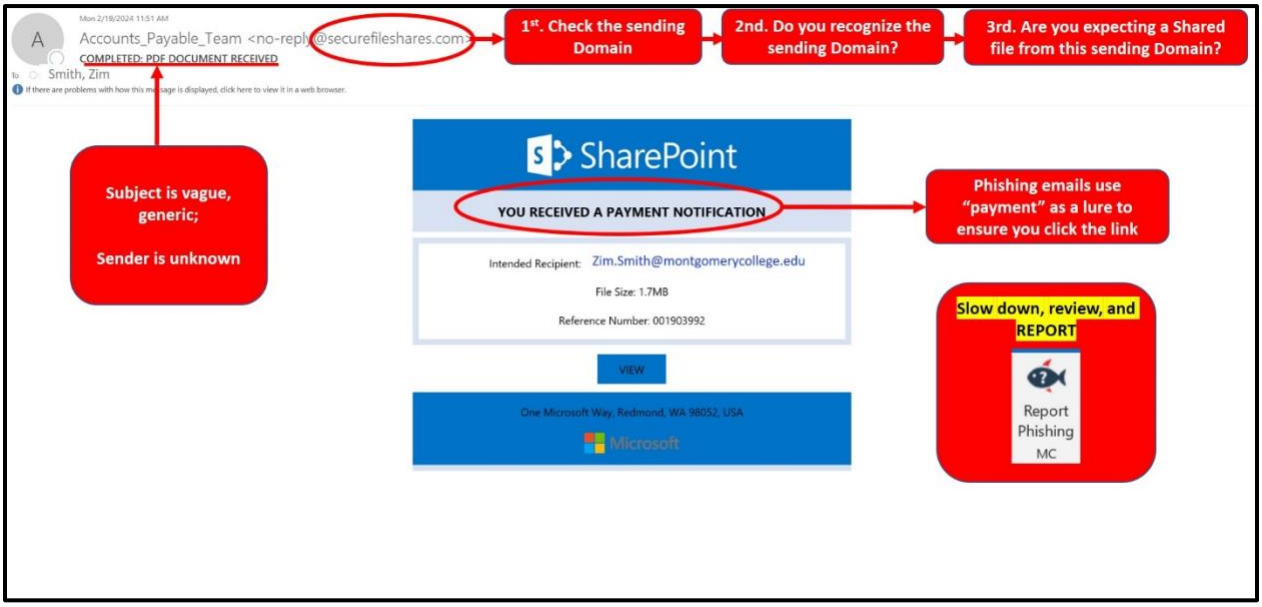
As part of our IT Security Awareness education program, OIT sent a simulated phishing scenario for February titled, *COMPLETED: PDF DOCUMENT RECEIVED*. This phishing scenario implied a "payment notification", a common tactic used to convince the recipient to click the link. Attackers use legitimate cloud storage or shared document platforms, such as SharePoint, to portray a legitimate email. Upon clicking the link, a fake login page is presented requesting your login username and password. Check out this Cofense article for an in-depth review of a file sharing phishing attack.

Be suspicious of emails sharing documents that you aren't expecting. Do not assume that emails sent using a legitimate service are safe. Stop, pause, and REPORT if you were NOT expecting a shared document. Don't allow your curiosity to take over.

Good news:
1142 employees reported the phishing scenario to the Phishtrap. Nice work MC!

Opportunities for improvement:
491 employees clicked the link within the training email. One is one too many – one click puts the entire MC network at risk!

Did YOU click? In a real-world phishing attack clicking the link may have prompted you to give up your login credentials. Please review the red flags within this type of phishing attack and learn 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 client allows you to quickly report suspicious emails to IT Security. Learn how to access the Phishing Reporter button when using Office 365 on the Web or from a mobile device.

As always, if you have any questions or concerns, please contact the IT Service Desk.