July Phishing Scenario Results

As part of our Security Awareness education program, the Office of Information Technology (OIT) sent a simulated phishing scenario titled, *#Incoming Restrict Messages# - Ref: KSK80508*. The phishing scenario notified the recipient that due to a server error, incoming messages have been restricted. The scenario provided a link to allow the recipient to "Recover Messages". Upon clicking the link, a look-alike Microsoft login page loads prompting the user to enter their login credentials. This type of email is designed to steal employee login credentials.

Remember, Montgomery College email filter notifications are sent from **MCSpamFilter@montgomerycollege.edu** and provide employees a link to "Manage My Account". Managing your quarantine, safe senders, and block senders list **does not** require you to login. Notifications from any other email address is a phishing attempt.

Good News

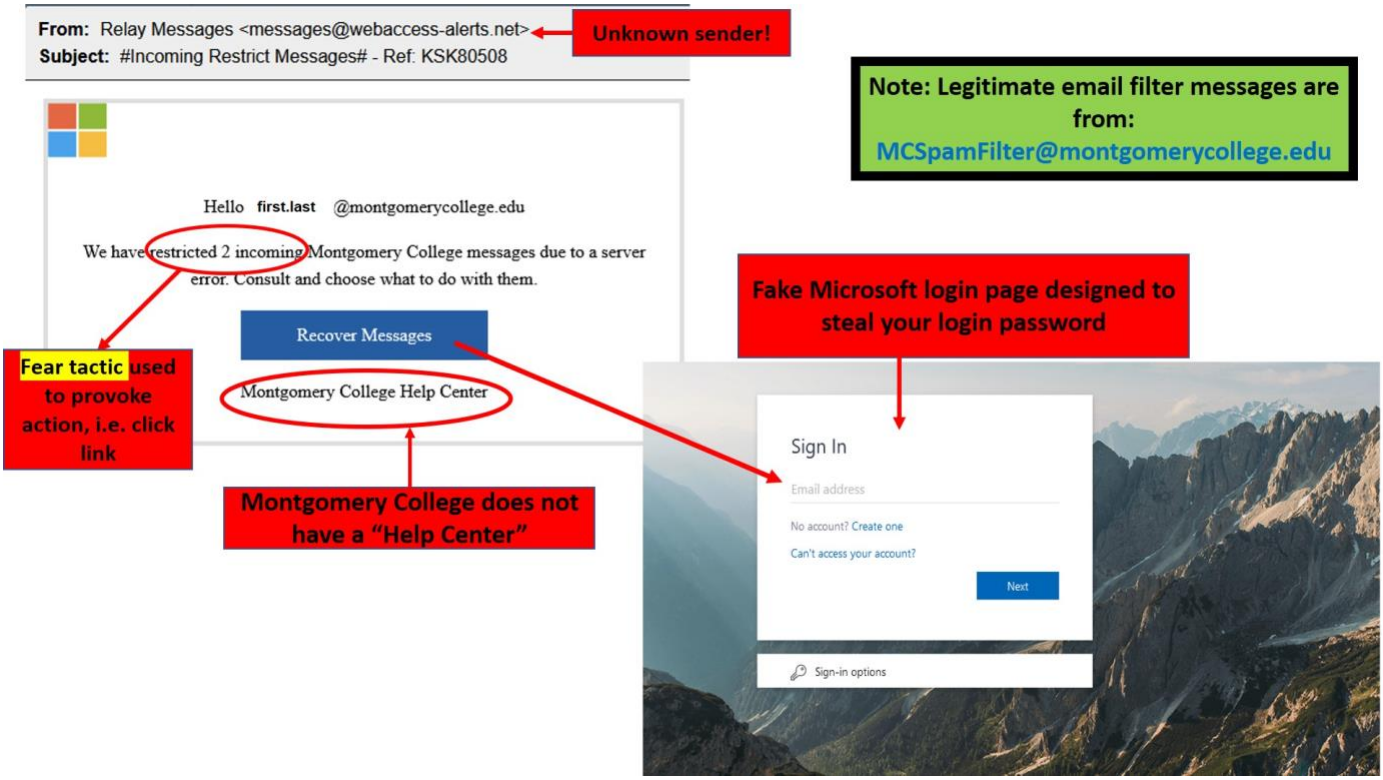
840 employees reported the phishing scenario to the Phishtrap. Keep up the good work!

Opportunities for Improvement

262 employees clicked the link within the training email; of these individuals, 29 entered their credentials.

Did you know that even ONE click puts the entire MC network at risk? 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 July phishing scenario to learn about this type of attack and ways to spot a suspicious email:



To avoid falling for these tricks remember to pause, reread the email, and if suspicious, **report the email using the Report Phishing button**.