April Phishing Scenario Results

As part of our Security Awareness education program, OIT sent a simulated phishing scenario titled, *Action Required: Update tax documents*. The phishing scenario notified the recipient that their "refund may be delayed" and to upload tax documents in the "Tax Center Portal".

This type of threat should be easy to detect, yet 275 employees clicked the link! To determine if the request is legitimate contact your tax preparer by phone to confirm as the legitimacy of the email is not determined by clicking the link.

It is best to organize your professional and personal communications by only using your Montgomery College email address for College business. This helps in identifying a phish/scam immediately since your tax provider would not be contacting you through your College email. To avoid falling for phishing attacks/scams review this helpful article from the Federal Trade Commission.

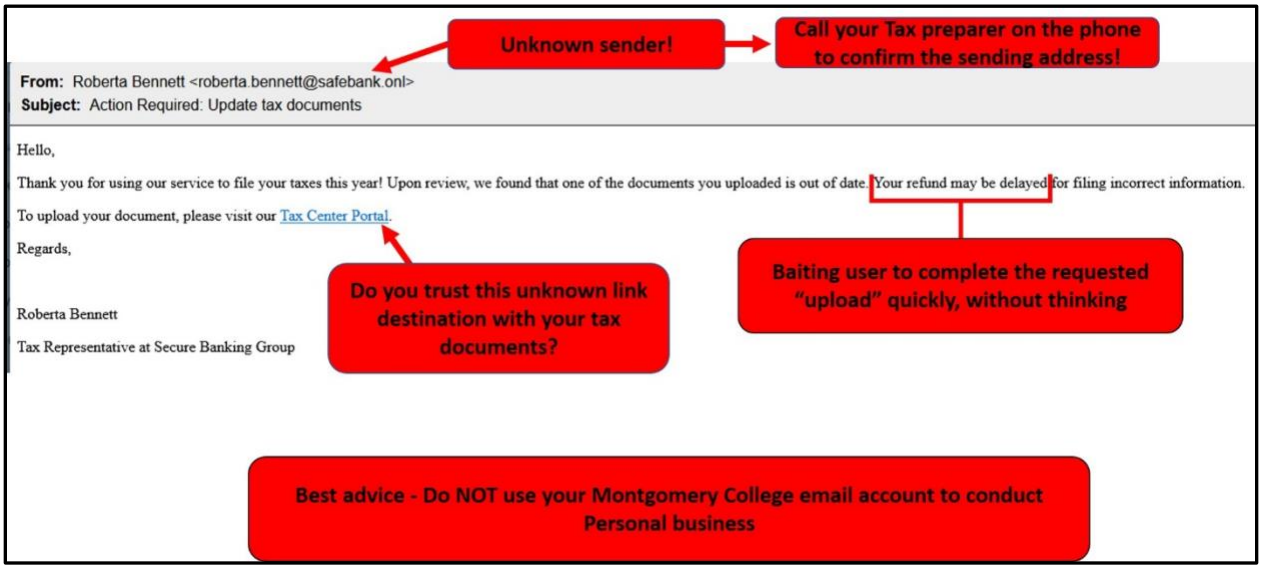
Good news:

1267 employees reported the phishing scenario to the Phishtrap. Keep up the good work!

Opportunities for improvement:

275 employees clicked the link within the training email. 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 April 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**.

Kindly direct technology-related questions or issues to the IT Service Desk:

- by email at itservicedesk@montgomerycollege.edu

- by web chat on OIT's web page
- by phone at 240-567-7222

Please do not reply to this email as this mailbox is not monitored. Thank you.

Sincerely,

IT Communications

Office of Information Technology