March 2025 Phishing Scenario Results:

As part of our Security Awareness Education Program, OIT sent a simulated phishing scenario titled, *An automatic Income tax Refund Notice*. The email indicated that “after our latest 12-monthly calculations…” you are eligible to receive an income tax return (we all have the honor of receiving an income tax return!). The notice provided a “password” and a link for the user to login.

Phishing attacks are most successful when a monetary offering or reward such as an income tax refund are promised. The prospect of receiving money is a trick to rush you into clicking the link without thinking through the request. This is where you need to pause and re-read the message. If it is too good to be true, it is probably a scam.

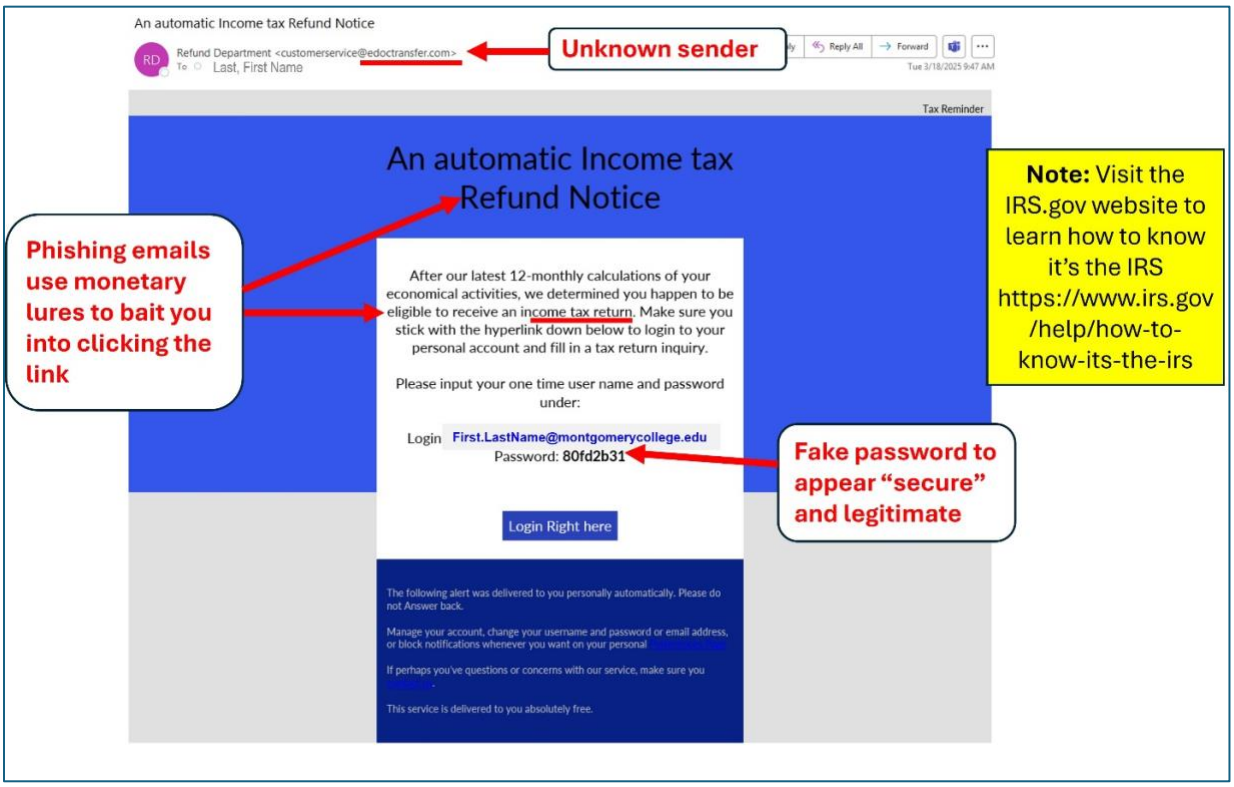
To avoid tax scams, make sure to ask your tax advisor their communication method and sending domain. This will prepare you in advance. Best practice is to use your personal email address for personal business! A tax notice email sent to your College email address is a dead giveaway. Lastly, review the IRS website on how to spot a scam and the ways they contact you.

Good News

1311 employees reported the phishing scenario to the Phishtrap. Nice work MC!

Opportunities for Improvement

45 employees clicked the link within the training email. 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 March phishing scenario to learn about this type of attack and ways to spot a suspicious email.



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.