Phishing Scenario Results: Payroll Scam

The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *Employee Notification Service*. This phishing scenario provided a link requesting the user to "…enable the service." The link in this type of threat often leads to a login page designed to mirror the College web login page (i.e., MyMC or M365). The purpose is to capture your login credentials and login to your account to change direct deposit information.

Learn to recognize the emotional triggers the attacker is using to trick you into clicking the link. In this scenario, the emotional trigger was excitement. The user may react to the emotional excitement of a possible increase in pay. Make your decision to click or report based on facts, not emotions. Remember, any update or information regarding your pay may be found by logging into your MC Workday account, not by clicking on a random link.

Good news:

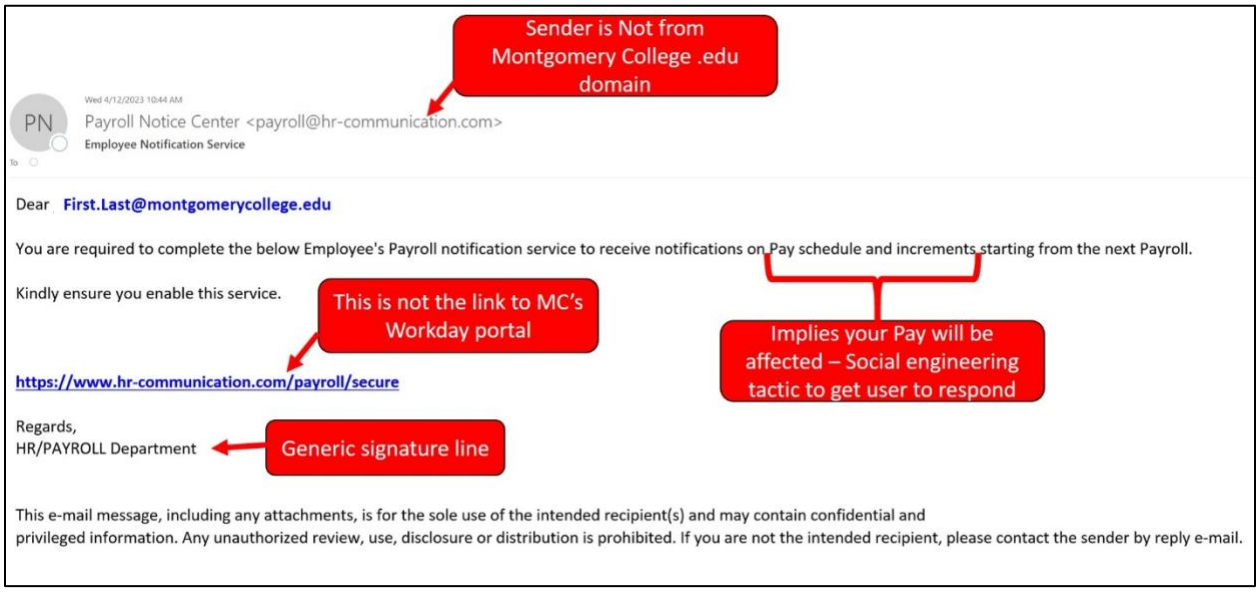
1126 employees reported the phishing scenario to the Phishtrap. Nice work MC!

Opportunities for improvement:

354 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 to 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 at home. If you accidentally clicked on a link or attachment in a suspicious email, contact the IT Service Desk immediately.

If you have any questions or concerns, please contact 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.