Phishing Scenario Results: Account Update
February 2023

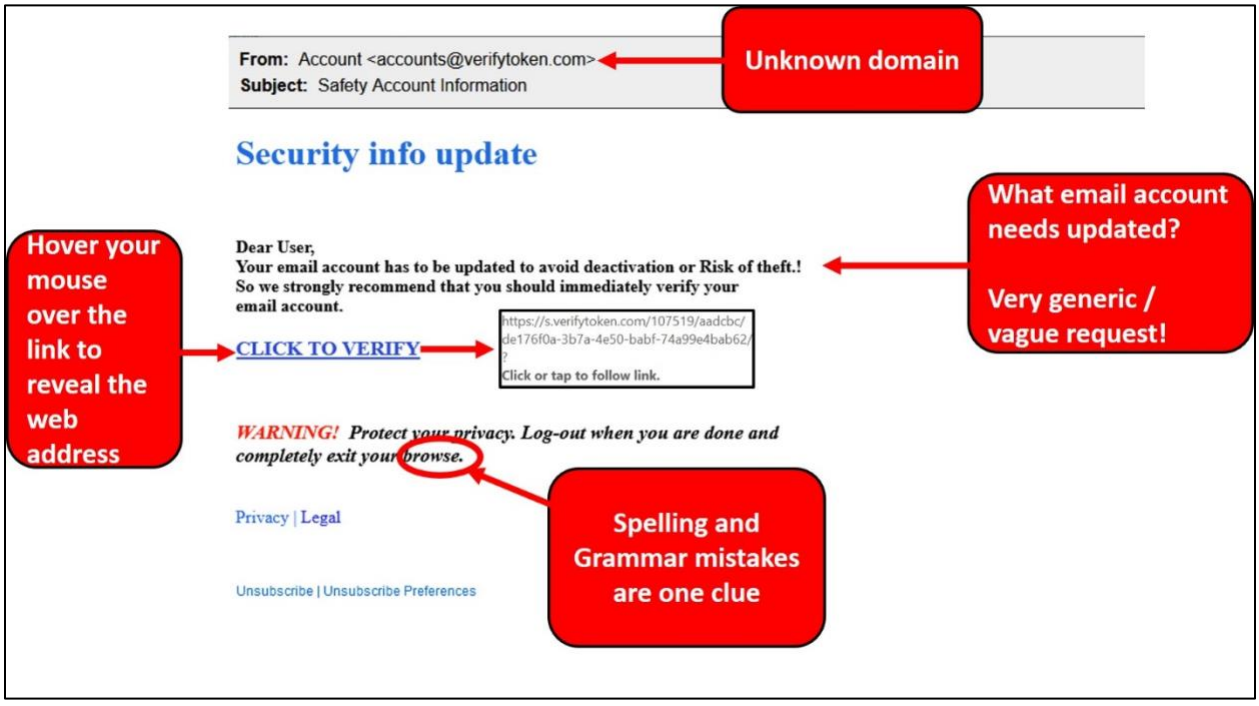
The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *Safety Account Information*. The email scenario directed the recipient to click a link to "verify" an email account. Account updates or verification request phishing emails are used as bait to capture login credentials. This is the easiest and most common social engineering trick used as no sophistication is required. The attacker simply "asks" for your login password. Your best defense is to report suspicious emails, especially requests for your account "verification"!

Good news: **978 employees reported** the phishing scenario to the Phishtrap. **Nice work MC!**

Opportunities for improvement: **20 employees clicked the link within the training email; of these individuals, 5 entered their credentials.**

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.

IT Communications
Office of Information Technology