Phishing Scenario Results: Update Mail Settings

The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *Settings Error*. The email requests the user to click the link to "automatically switch to the new email…" Emails directing employees to update "mail settings" via an included link are designed to steal login credentials.

Remember, IT changes or updates are announced from the ITCommunications@montgomerycollege.edu sending address, and major upgrade announcements provide an MC website for more information. Always safeguard your MC login credentials and question out of ordinary requests.

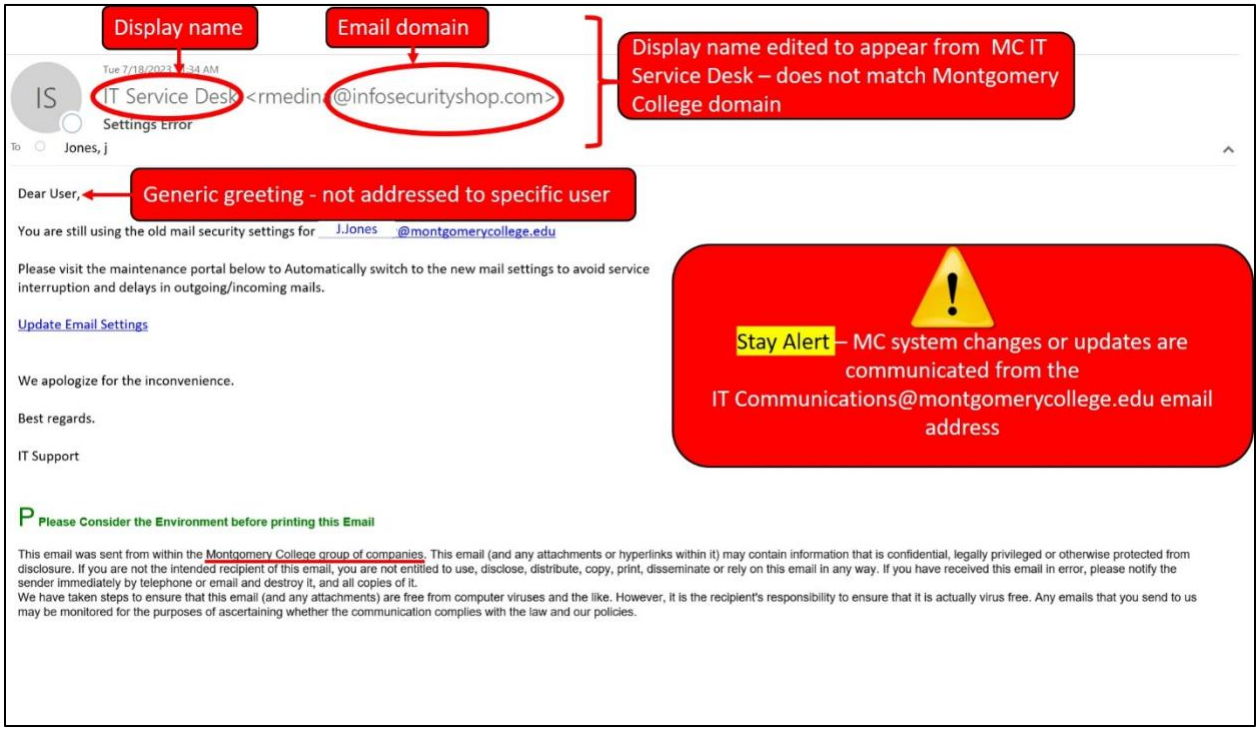
Good news:

1,060 employees reported the phishing scenario to the Phishtrap. **Nice work MC!**

Opportunities for Improvement:

334 employees clicked the link within the training email. One click 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.

IT Communications
Office of Information Technology