January 2024 Phishing Scenario Results: QR Codes

Our January phishing scenario introduced Quick-Response (QR) code phishing scams. The scenario was titled, *Please verify your email address*, and provided a QR code directing the user to "finish your email address verification…" by scanning the QR code. QR codes provide a layer of cover and may be less transparent to the recipient. They often embed a malicious web address with the intent of capturing your login credentials. Please review this informative SANS article to learn more about the dangers and how to safely use/receive QR codes.

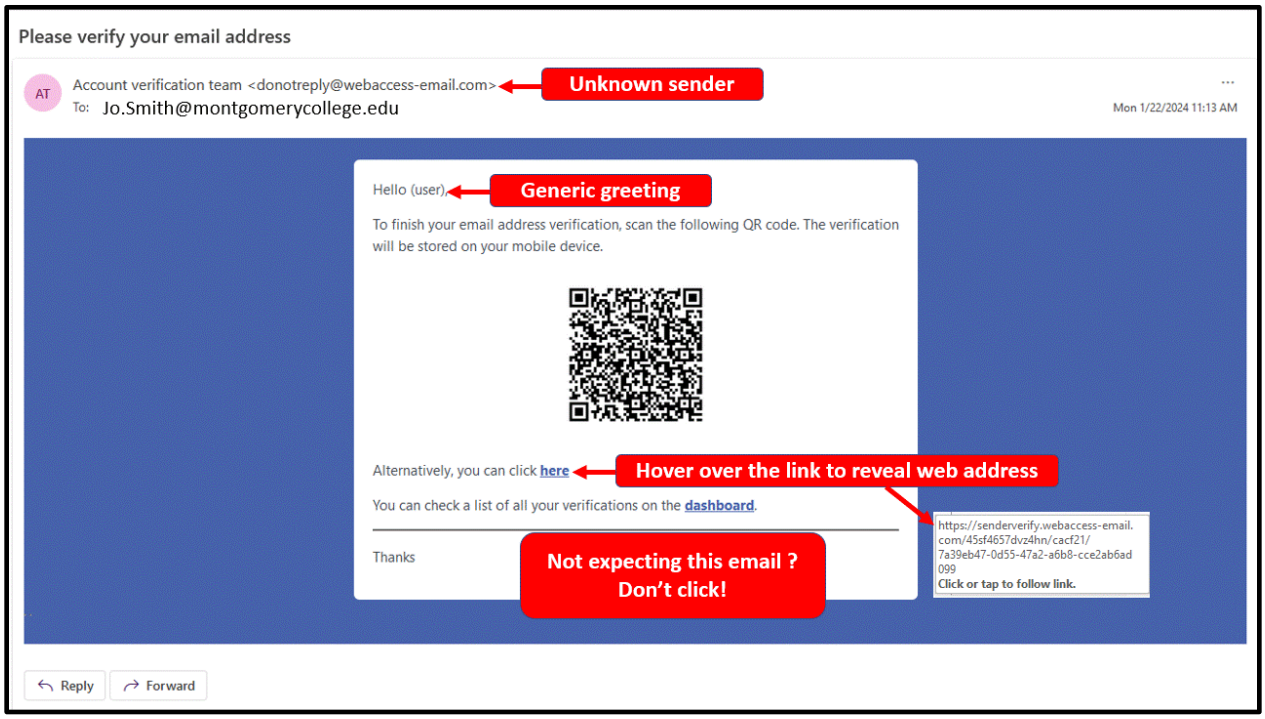
Remember, IT changes or updates are announced from the ITCommunications@montgomerycollege.edu sending address, and major upgrade announcements provide an MC website for more information. Always safeguard your MC login credentials and question unusual requests.

Good News:
1,160 employees reported the phishing scenario to the Phishtrap. **Nice work MC!**
Opportunities for Improvement:

90 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.