Phishing Scenario Results: File Transfer

The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *noreply <noreply@premiumisp.net> sent you files Montgomery College WeTransfer*. This phishing scenario implied an established business relationship with Montgomery College and the need to "resolve" the issue. Both are purposeful tactics used to trick you into clicking the link.

Learn about social engineering tactics to avoid being tricked, and most importantly, follow MC business processes when ordering products, expecting deliveries, and approving invoices.

Good news:

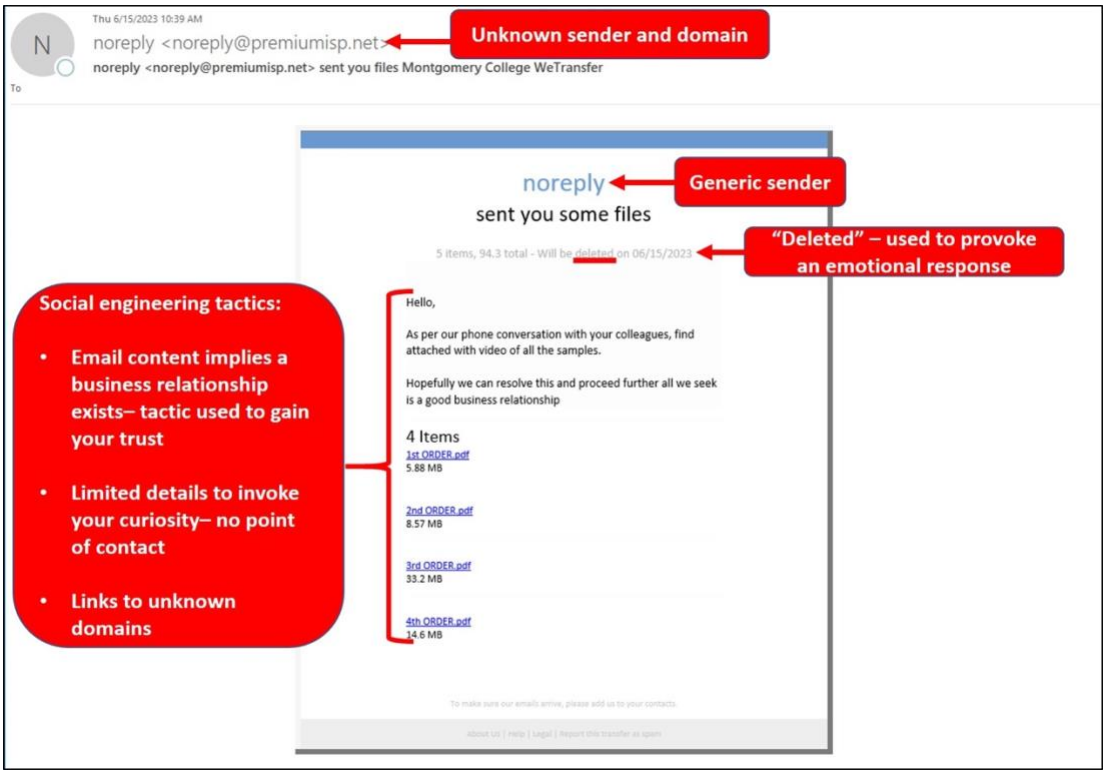
1,005 employees reported the phishing scenario to the Phishtrap. **Nice work MC!**

We are making progress:

46 employees clicked the link within the training email; of these individuals, 2 entered their credentials. Our numbers are getting better, but 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.