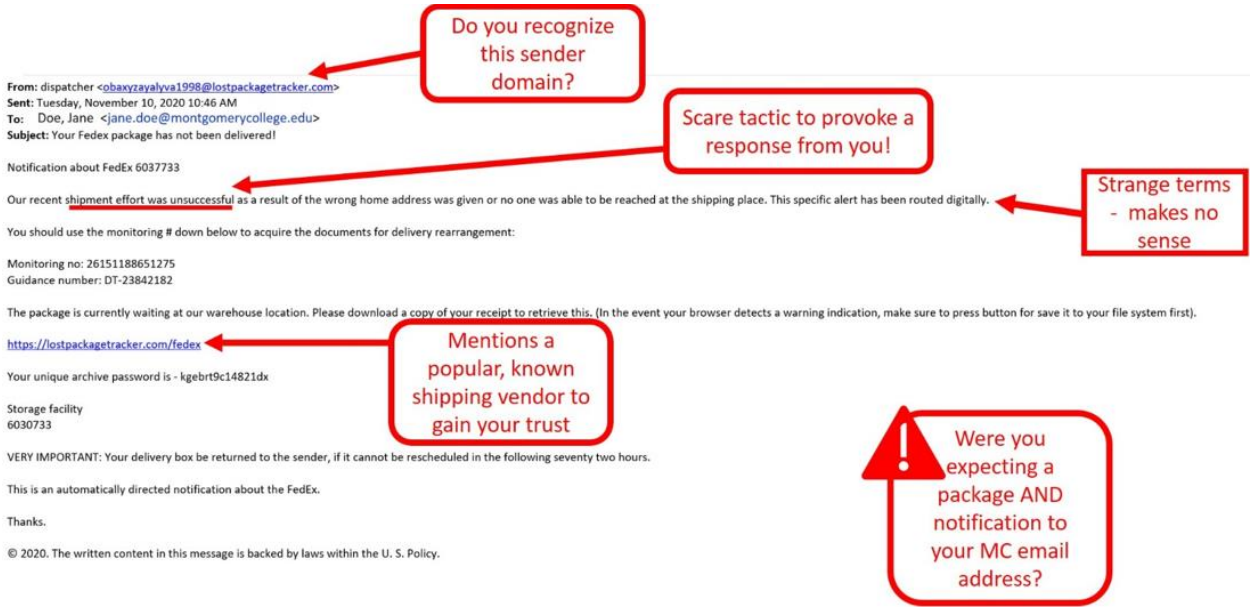
November 2020 Phishing Scenario Results: Package delivery/shipping notifications

The Office of Information Technology (OIT) recently completed a phishing scenario with the subject, "*Your Fedex package has not been delivered!".* An email like this is guaranteed to grab your attention, especially during this remote situation. This educational scenario shows how attackers are continuously evolving and in this seasonal tactic, they take advantage of the deluge of emails by sending creative package delivery phishing emails designed to catch you off guard.

1,001 employees reported the FedEx package themed phishing email! Thanks to these employees, IT Security would have the time advantage it needs to respond to potential threats.

136 employees clicked the link within the training email. Check out the clues within the email to help you identify this email as suspicious:



What should you do if you suspect an email may be a phishing attempt?

REPORT the email! Educated employees are our last line of defense to thwart phishing attacks and help us prevent data breaches. 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.

Complete (or revisit) DataSecurity@MC: Annual Review!

DataSecurity@MC: Annual Review training provided by SANS will teach you how to better identify common methods used by cyber attackers who try to gain access to account credentials and information systems. The range of training topics takes about 35 minutes to complete and can be accessed through MC Learns.

Below are some common clues to look for in identifying a suspicious email:

- Be wary of some of these popular narratives used in shipping emails: Failed delivery, Invoice, Request for quote, Package notification, Confirm shipping address, Status update.
- Check your emotions. Beware of emotional triggers such as lost or delayed package.
- Organize and keep track of your online orders - use your personal email address for personal business.
- Be cautious. Malicious actors and aggressive spammers are attempting to take advantage of our new normal by **preying on our stress levels and hoping our guard is down with COVID-19**, gift card, meeting invites, shipping notices, and stimulus check scams.
- Trust your instincts**.** If the email content, sender, and link or email attachment seems suspicious, do not open it. Play it safe and REPORT it.
- Remember, phishing emails are the preferred method among attackers because it is the easiest way to get your login credentials. Don't give them the opportunity.
- The message is overly generic, the request is outside of your scope of responsibility, and/or the action requested is not typical of a current business process.

If you have any questions or concerns regarding this process, 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