Phishing Results – November 2021

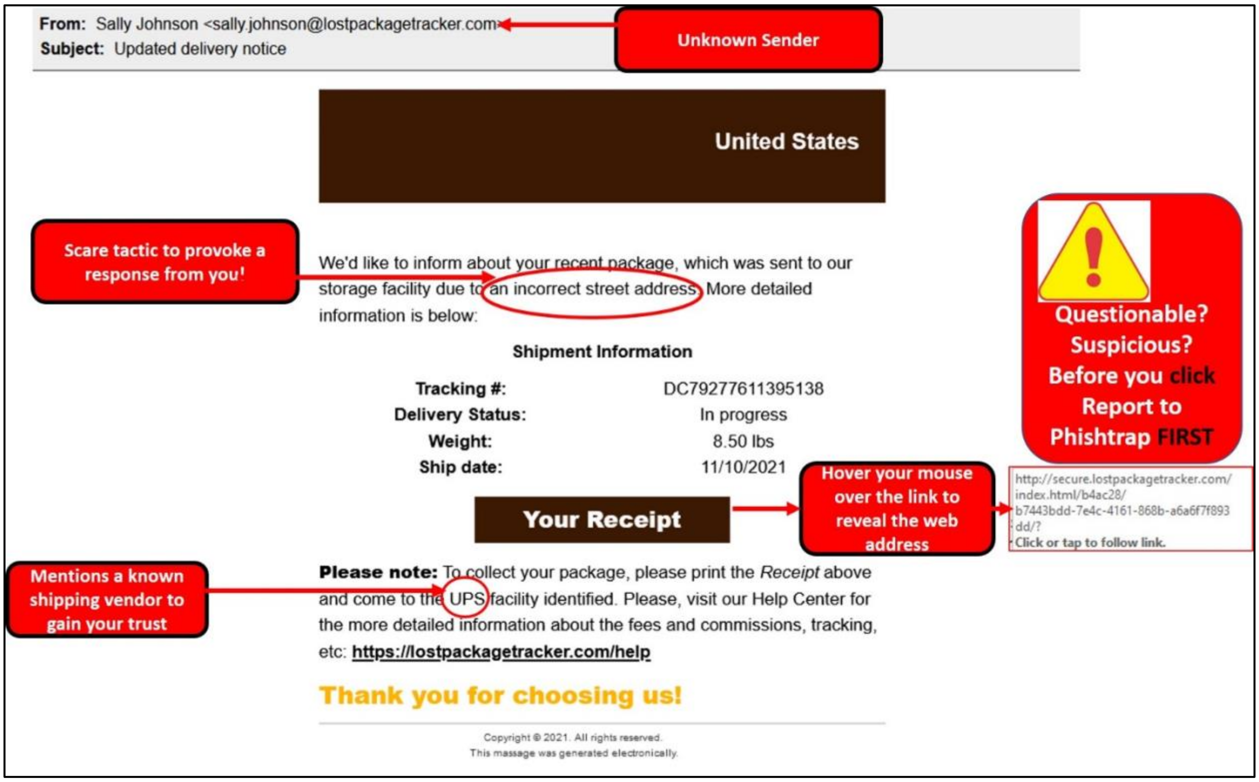
The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *Updated delivery notice*, with a link to "Your Receipt". Package delivery notices are a common threat during the holiday season and in this case the "incorrect street address" message invokes an emotional response to get the recipient to act – click the link.

1041 employees reported the phishing scenario to the Phishtrap. **Good job MC!**

184 employees clicked the link within the training email. In a real phishing incident, those 184 employees would potentially allow:

- Access to MyMC accounts
- Sensitive College data to be breached
- Ransomware to be introduced to workstations and other key systems
- Disruption to College business

Please review the red flags within this type of phishing attack:



From: Sally Johnson <sally.johnson@lostpackagetracker.com>
Subject: Updated delivery notice

United States

We'd like to inform about your recent package, which was sent to our storage facility due to an incorrect street address. More detailed information is below:

Shipment Information

Tracking #:	DC79277611395138
Delivery Status:	In progress
Weight:	8.50 lbs
Ship date:	11/10/2021

Your Receipt

Please note: To collect your package, please print the *Receipt* above and come to the UPS facility identified. Please, visit our Help Center for the more detailed information about the fees and commissions, tracking, etc: **https://lostpackagetracker.com/help**

Thank you for choosing us!

Copyright © 2021. All rights reserved.
This massage was generated electronically.

http://secure.lostpackagetracker.com/index.html/b4ac28/b7443bdd-7e4c-4161-868b-a6a6f7f893dd/?
Click or tap to follow link.

Unknown Sender
Scare tactic to provoke a response from you!
Questionable? Suspicious? Before you click Report to Phishtrap FIRST
Hover your mouse over the link to reveal the web address
Mentions a known shipping vendor to gain your trust

Report
Phishing
MC

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 Outlook allows you to quickly report suspicious emails to IT Security.

If using Office 365 on the web, follow these steps to pin the Reporter Button to your email message surface. 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 in MC Learns through Workday under the **MC Required Training** category.

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

- Think twice. Read emails thoroughly. DO NOT use your College email for personal business. Set up your Amazon and other personal accounts with a personal email address!
- Go to the source – if you are expecting a delivery (College business or personal) go to the delivery carrier's website directly or use the retailer's tracking tools.
- Check your emotions. Do not be curious and investigate the link – **REPORT** the email.
- 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.

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