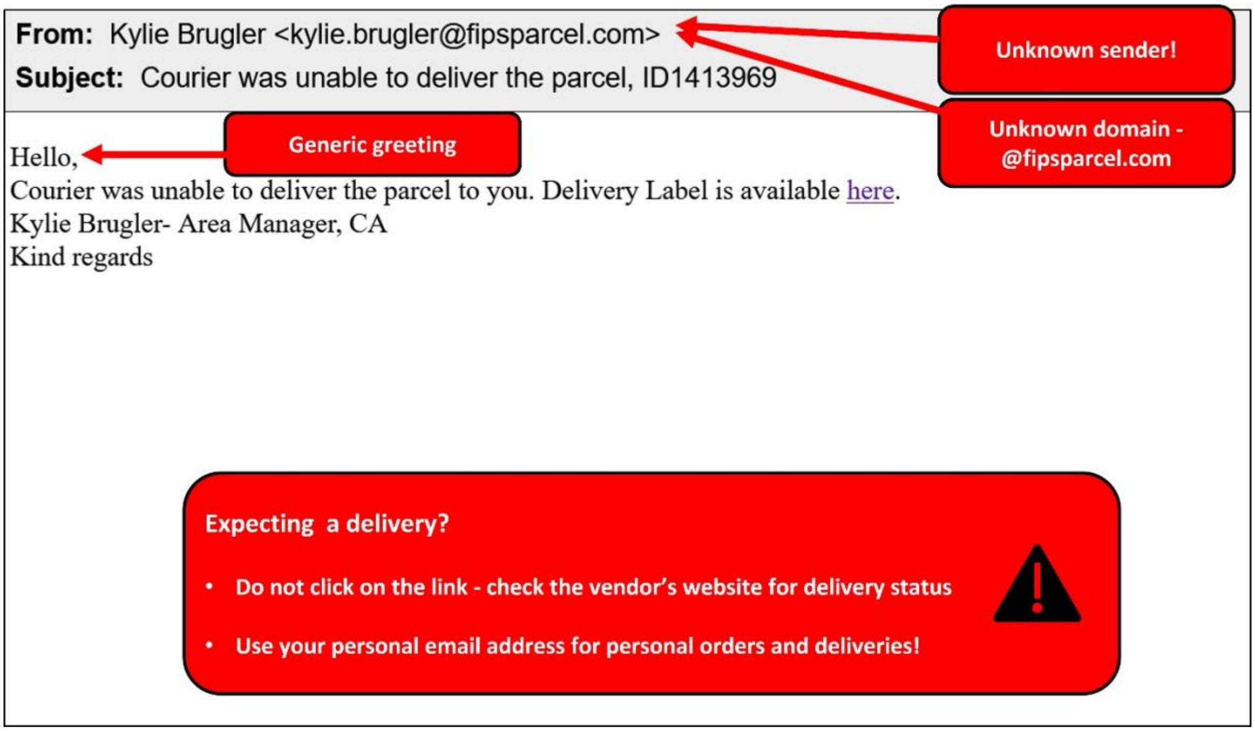
**March Phishing Results: Package Delivery Malware Threat**

The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *Courier was unable to deliver the parcel, ID1413969*. This email contained limited information such as the courier's name and package order. The expectation is the recipient will click the link in search of more information on the order. This lack of detail and generic greeting are tactics attackers use to lure the recipient into clicking the link. This is one way malware is delivered. Do not try to investigate – report the email!

**1086 employees reported** the phishing scenario to the Phishtrap. **Nice work MC!**

**168 employees clicked the link within the training email.** There were several clues within the email to help you identify this message as suspicious. Please review the red flags below:



**From:** Kylie Brugler <kylie.brugler@fipsparcel.com>
**Subject:** Courier was unable to deliver the parcel, ID1413969

Hello,
Courier was unable to deliver the parcel to you. Delivery Label is available here.
Kylie Brugler- Area Manager, CA
Kind regards

Unknown sender!

Unknown domain - @fipsparcel.com

Generic greeting

Expecting a delivery?

- Do not click on the link - check the vendor's website for delivery status
- Use your personal email address for personal orders and deliveries!

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 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 in MC Learns through Workday under the **MC Required Training** category.

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

- If you are expecting a package contact the delivery service or seller directly using a verified number or website.
- Keep your MC business limited to your MC email address and use your personal email address for personal business.
- Always verify! If you know the sender, but the email seems out of context, follow up with a quick phone call.
- 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.