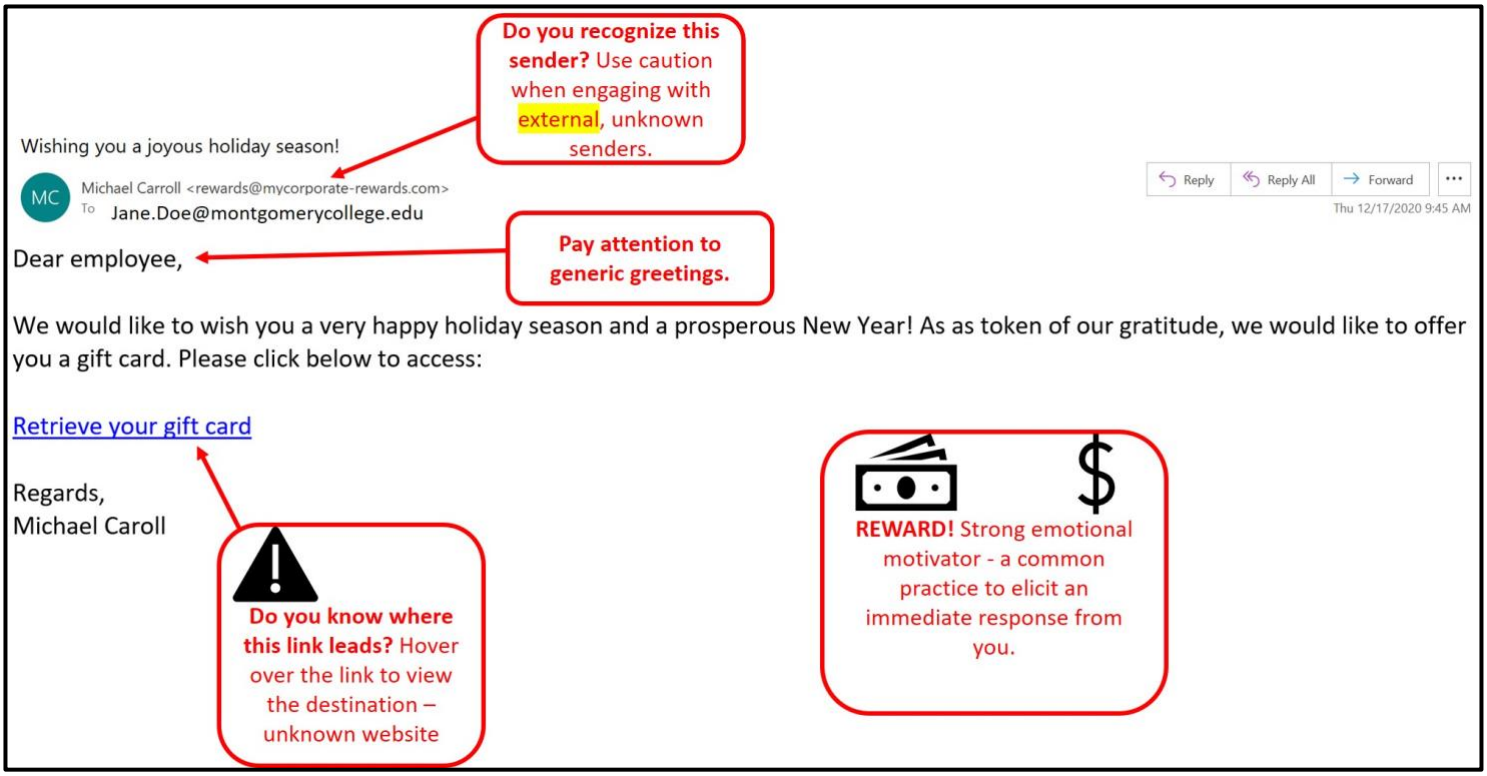
December 2020 Phishing Scenario Results

The Office of Information Technology (OIT) continuously strives to educate employees on phishing threats using mock scenarios. The December 2020 phishing scenario titled, "Wishing you a joyous holiday season" resembles a common phishing email used by attackers to distribute **malware**. The lure used in this type of scam is a gift card. Rewards or something free are strong emotional motivators that often catch us off-guard.

820 employees reported the holiday gift card email! Thanks to these employees, IT Security would have the time advantage it needs to respond to potential threats.

118 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 in MC Learns through Workday.

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

- Be wary of emails from unknown senders, especially of those sending you a Gift! Do you send gifts to people you do not know?
- Check your emotions. Beware of emotional triggers such as “reward” or “gift cards”.
- 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.
- Another red flag - 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