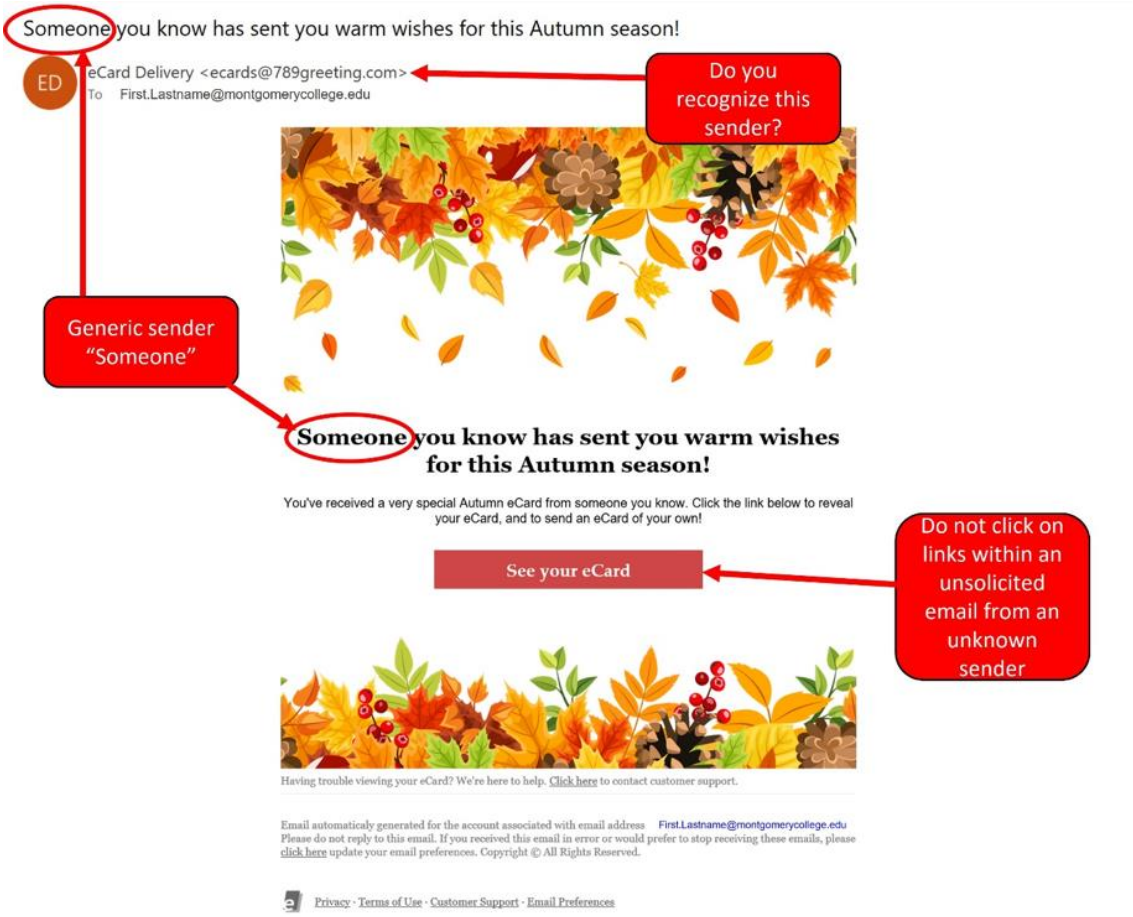
The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *Someone you know has sent you warm wishes for this Autumn season*, with a link to "See your eCard". Electronic greeting cards (eCards) are easy to create and provide an inexpensive way to send greetings to family and friends. Unfortunately, scammers use eCards as well. The most common threat associated with an eCard is an employee clicking the link or attachment and downloading spyware, malware, or a computer virus.

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

341 employees clicked the link within the training email.

Please review the scenario and clues:



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:

- A generic eCard from "Someone" is a red flag. Any email from an unknown sender using a free eCard service is not worth your time.
- Only use your Montgomery College email address for College business. This helps you organize your known contacts and distinguish between personal and business email sending addresses.
- Check your emotions. Do not be curious and investigate the link – **REPORT** the email!
- 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.

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