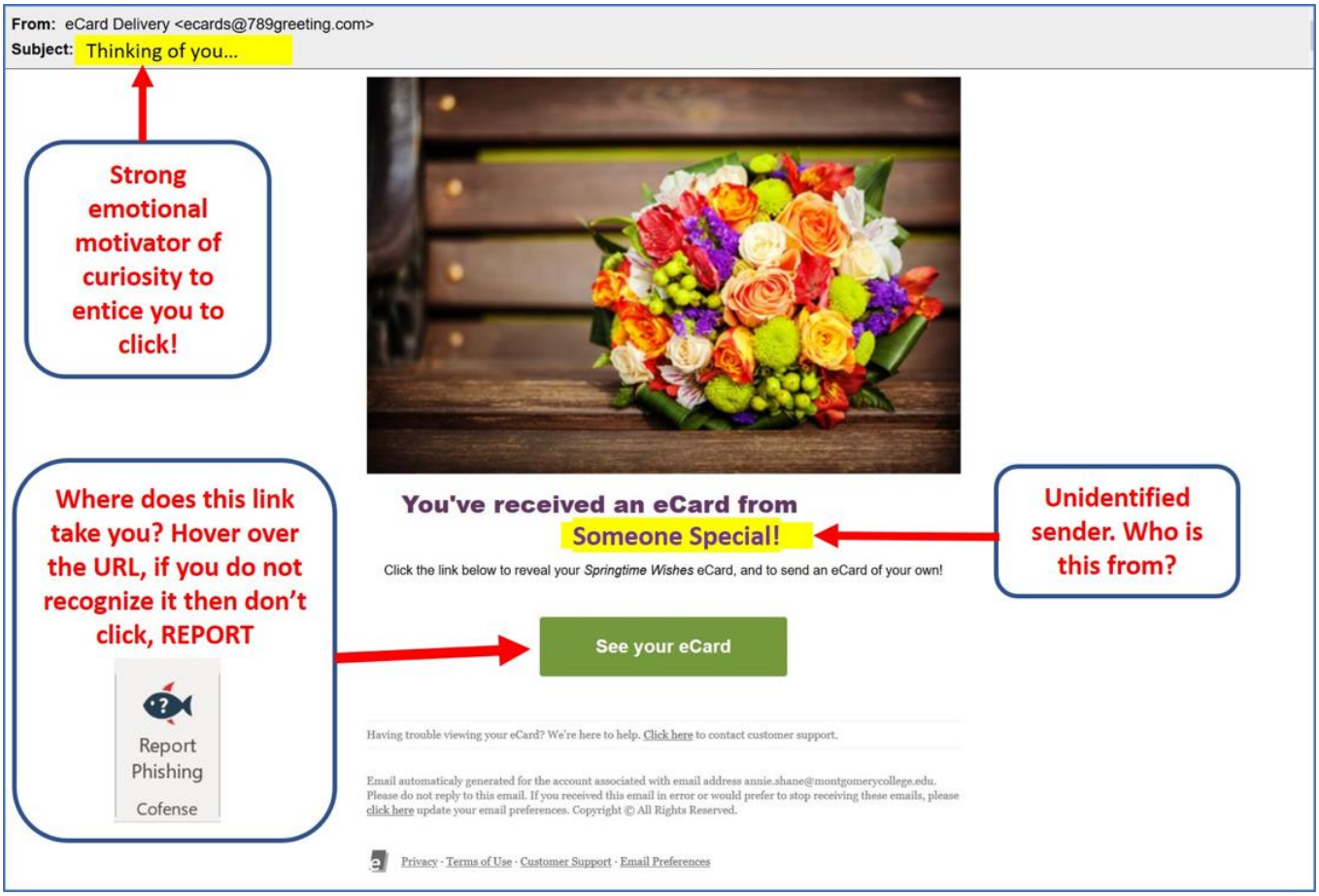
April 2020 Phishing Exercise Recap: Vulnerability at Home
April 28, 2020

The Office of Information Technology (OIT) recently completed a simulated phishing training exercise, which prompted users to click a link in order to retrieve a “Spring eCard”. This simulation is a reminder of how attackers try to gain your trust using enticing greetings and graphics to lure employees into clicking on unknown links.

Typically, we see more reporters than clickers, but this month those numbers were reversed. This demonstrates how much more vulnerable we are when working from home with distractions, leaving us open to attacks by bad actors looking to take advantage. Please stay vigilant when reviewing email. Stay safe online!

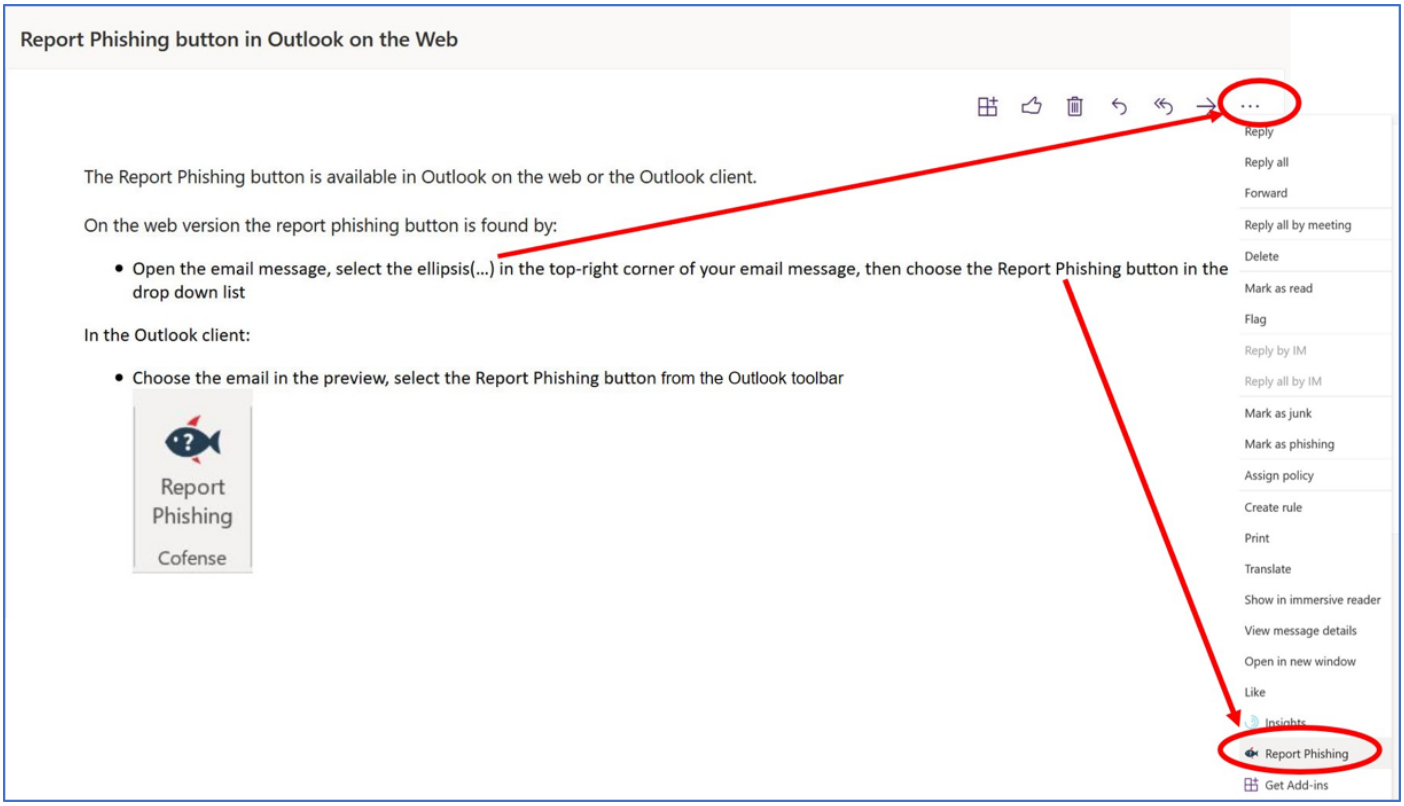
534 employees reported this simulated phishing email without falling susceptible to the training email. Thanks to these employees, IT Security would have the time advantage it needs to respond to potential threats.

806 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 email again and pay close attention to the red flags:



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

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. If you suspect an email is malicious, or you have accidentally clicked on a link or attachment in a suspicious email, use this button to report the email immediately.



Complete the Data Security @MC training within MC Learns

Data Security@MC 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. This training will also provide tips and techniques to help detect and defend against these threats. The range of training topics takes about 35 minutes to complete. Below are some common clues to look for in identifying a suspicious email:

- The email has no identifying characteristics, such as corporate branding, valid contact information, or known sender information.
- 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.

- The email includes an urgent deadline for completion or a severe consequence if the request is not complete - i.e. Follow MC processes and procedures
- The email uses strong emotional messaging - 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**, gift card, and stimulus check scams.
- Trust your instincts**.** If the email content, sender, and link or email attachment seems suspicious, don't open it, play it safe and REPORT it.