February 2020 Phishing Exercise Recap: Shared Outlook Calendar
February 27, 2020

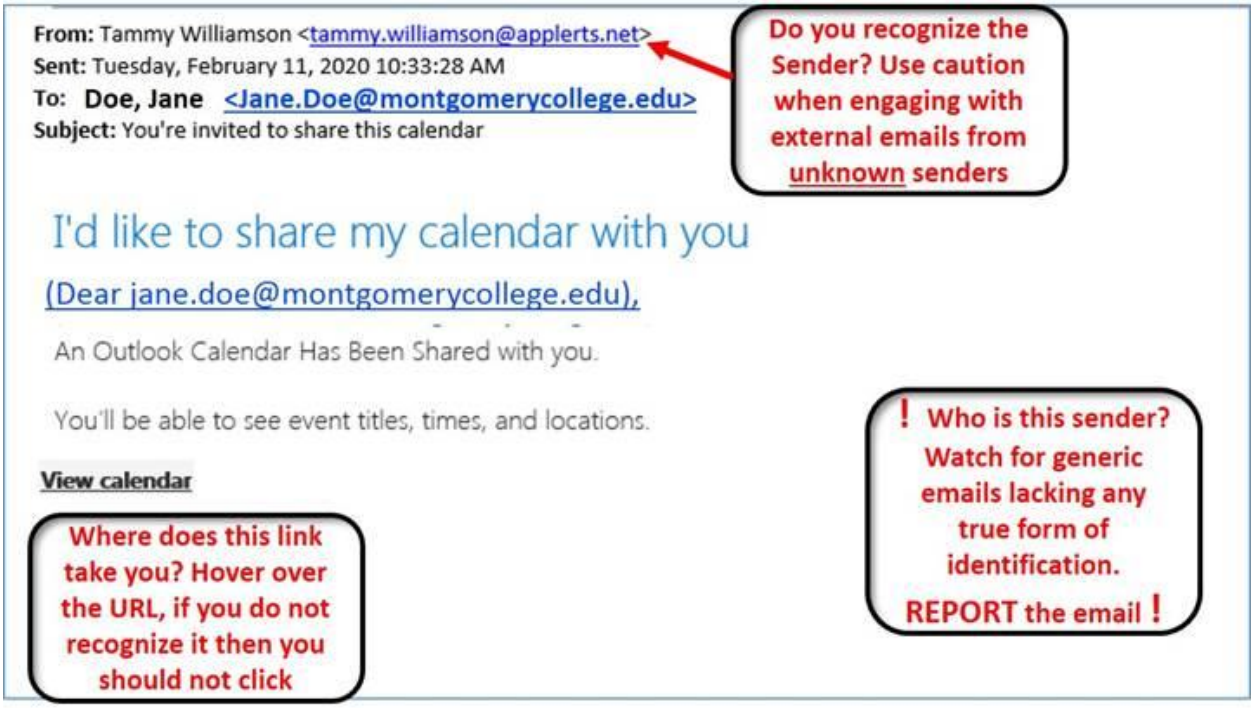
Montgomery College recently completed a simulated phishing training exercise, which prompted users to click a link in an email in order to view a shared Outlook calendar. This exercise simulated a common tactic – invoke a sense of curiosity in the recipient. Malicious actors use emotional cues to provoke a response.

645 Montgomery College employees reported this simulated phishing email without falling susceptible to the training email.

That is up 6% from last month's training exercise. Thanks to these employees, our security team would have the time advantage it needs to respond to potential threats!

245 Montgomery College employees clicked the link within the training email.

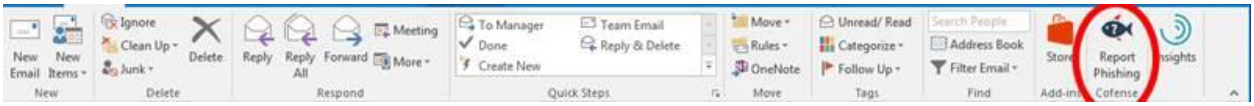
There were several clues within the email to help you identify this message as suspicious. Please review the email again and pay close attention to the red flags:



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

When technical controls fail, 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 report suspicious emails to our security team with

just one click. 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:

1. The email originates from outside the Montgomery College network and spoofs an internal style of communication – i.e. tammy.williamson**@applerts.net**
2. The email has no identifying characteristics, such as corporate branding, valid contact information, or known sender information.
3. 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.
4. The email includes an urgent deadline for completion or a severe consequence if the request is not complete.
5. The email uses strong emotional messaging to encourage you to click, such as curiosity, fear, and urgency.
6. Spelling and grammatical errors are present.

While this list is not all-inclusive, you will typically find 2-3 of these tactics used in a phishing attack.