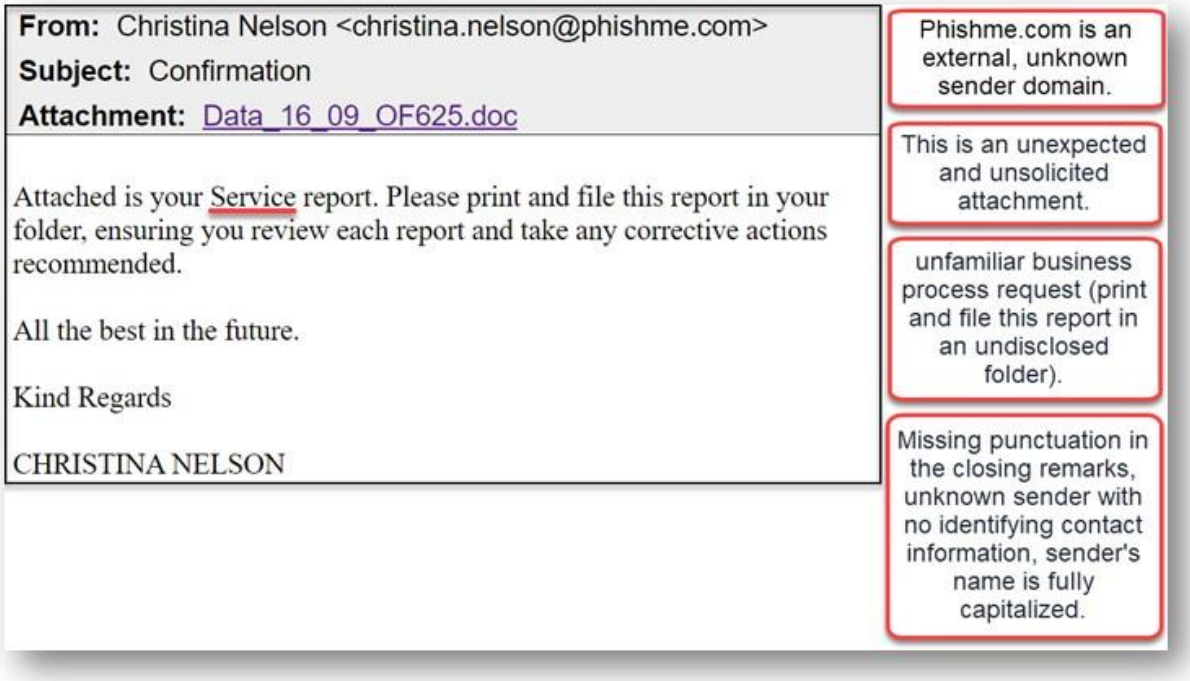
November 2019 Phishing Exercise Recap: Service Report File
November 25, 2019

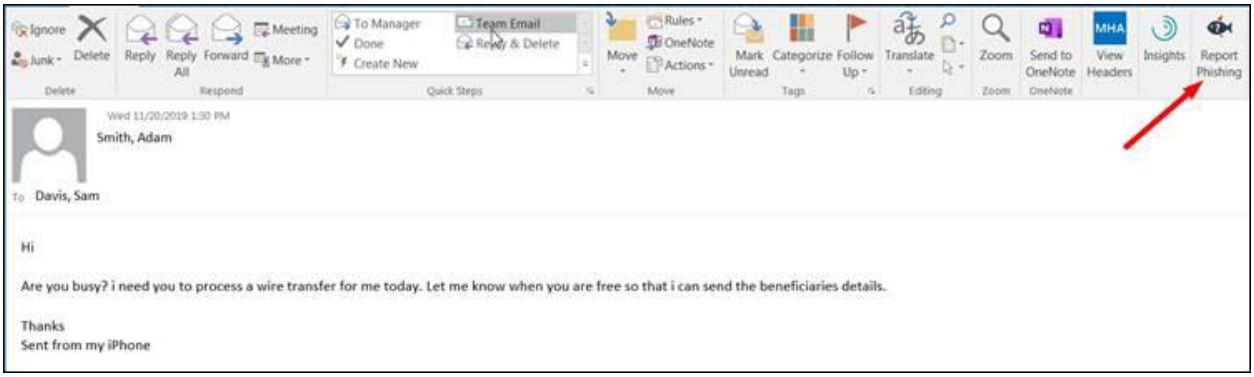
The Office of Information Technology (OIT) recently completed a simulated phishing training exercise, which prompted users to open a service report file titled, Data_16_09_OF625.doc. This exercise was designed to give you a realistic phishing experience in a safe and controlled environment. Doing so, allows you to become more familiar and more resilient to the tactics used in real phishing attacks.

292 Montgomery College employees opened the attachment. 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. The "Report Phishing" button within your email client allows you to quickly report suspicious emails to IT Security with just one click! If you suspect an email is malicious use this button to report the email immediately.



821 Montgomery College employees reported this simulated phishing email without opening the attachment. Thanks to these employees, our security team would have the time advantage it needs to respond to potential threats!

Not all malicious emails will look the same, but you can identify many by watching for these clues:

1. The email originates from outside the Montgomery College network and spoofs an internal style of communication.
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, urgency.
6. Spelling and grammatical errors are present.

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

Take the required Data Security training available through MC Learns.

Data Security@MC training modules are located in the Required Training section and must be completed by June 30, 2020.