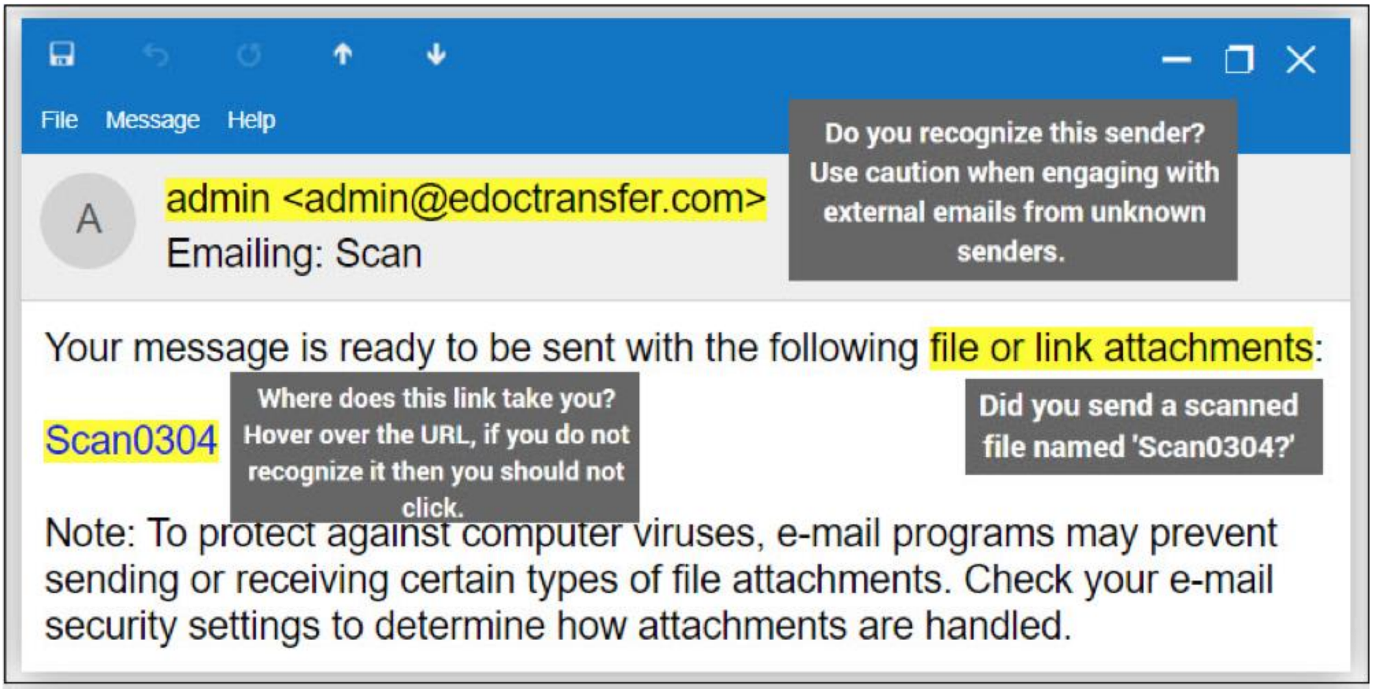
January Phishing Exercise Recap: Sending a Scan
February 10, 2020

Montgomery College recently completed a simulated phishing training exercise, which prompted users to click a link to preview a scanned document. 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.

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

193 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:



admin <admin@edoctransfer.com>
Emailing: Scan

Do you recognize this sender? Use caution when engaging with external emails from unknown senders.

Your message is ready to be sent with the following file or link attachments:

Scan0304

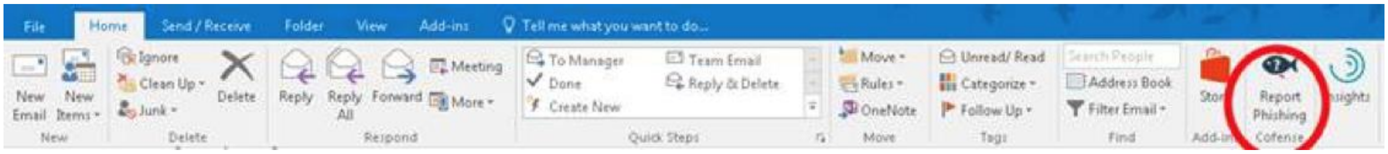
Where does this link take you? Hover over the URL, if you do not recognize it then you should not click.

Did you send a scanned file named 'Scan0304?'

Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.

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 quickly report suspicious emails to our security team with just one click! If you suspect an email is malicious, use this button to report the email.



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.

Reminder: Complete the Data Security @MC required training by June 30, 2020.
The 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.