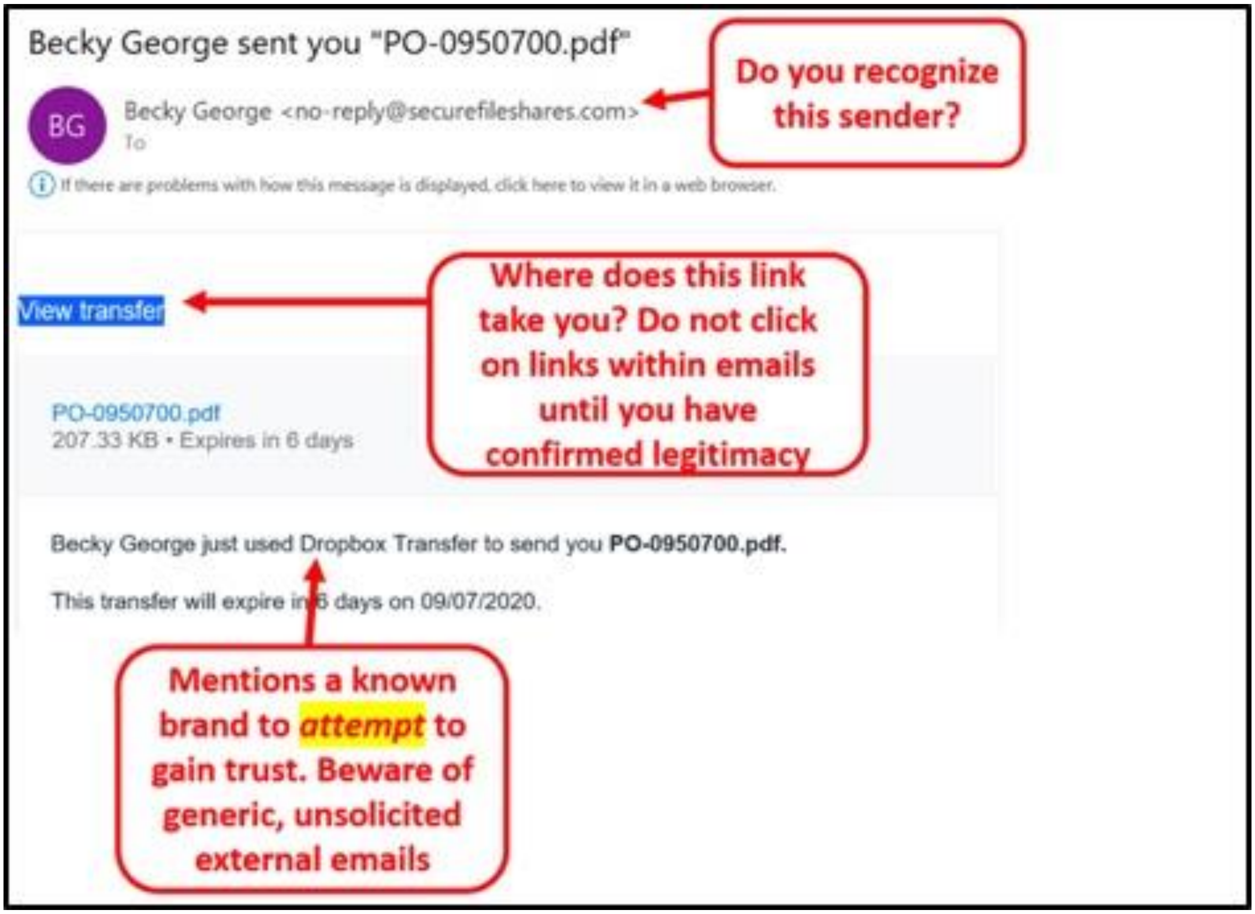
September 2020 Phishing Scenario Results: Shared Dropbox File

The Office of Information Technology completed a simulated phishing training exercise, which prompted users to click a link to download a shared Dropbox file. This is a common method used by attackers to capture your credentials. Cloud sharing programs help facilitate our business processes. Beware and report unsolicited emails that contain a link to share files. If you do not know the person, do not click on the link.

939 employees reported the phishing scenario email, *Becky George sent you PO-0950700.pdf*. Thanks to these employees, IT Security would have the time advantage it needs to respond to potential threats.

42 employees clicked the link AND entered their MyMC credentials within the training email. In a real phishing email, this would provide an attacker complete access to your MyMC and Office 365 email accounts!

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



Becky George sent you "PO-0950700.pdf"

BG Becky George <no-reply@securefileshares.com>

To

If there are problems with how this message is displayed, click here to view it in a web browser.

View transfer

PO-0950700.pdf
207.33 KB • Expires in 6 days

Becky George just used Dropbox Transfer to send you **PO-0950700.pdf.**

This transfer will expire in 6 days on 09/07/2020.

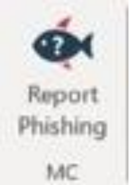
Do you recognize this sender?

Where does this link take you? Do not click on links within emails until you have confirmed legitimacy

Mentions a known brand to *attempt* to gain trust. Beware of generic, unsolicited external emails

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. Learn how to access the Phishing Reporter button when using Office 365 at home. 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 through MC Learns.

Below are some common clues to look for in identifying a suspicious email:

- Remote work has increased our usage of cloud sharing technologies. When communicating with outside parties about file sharing **ask in advance** what cloud sharing platform they use and who will be sending the email.
- Check your emotions. Beware of emotional triggers such as an urgent deadline for completion or severe consequences if the request is not complete -i.e. follow MC processes and procedures.
- 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, 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.
- The email has no valid contact information or known sender information. Do not accept a conference invite from an unknown sender.
- 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.

For any technology-related questions or issues, 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