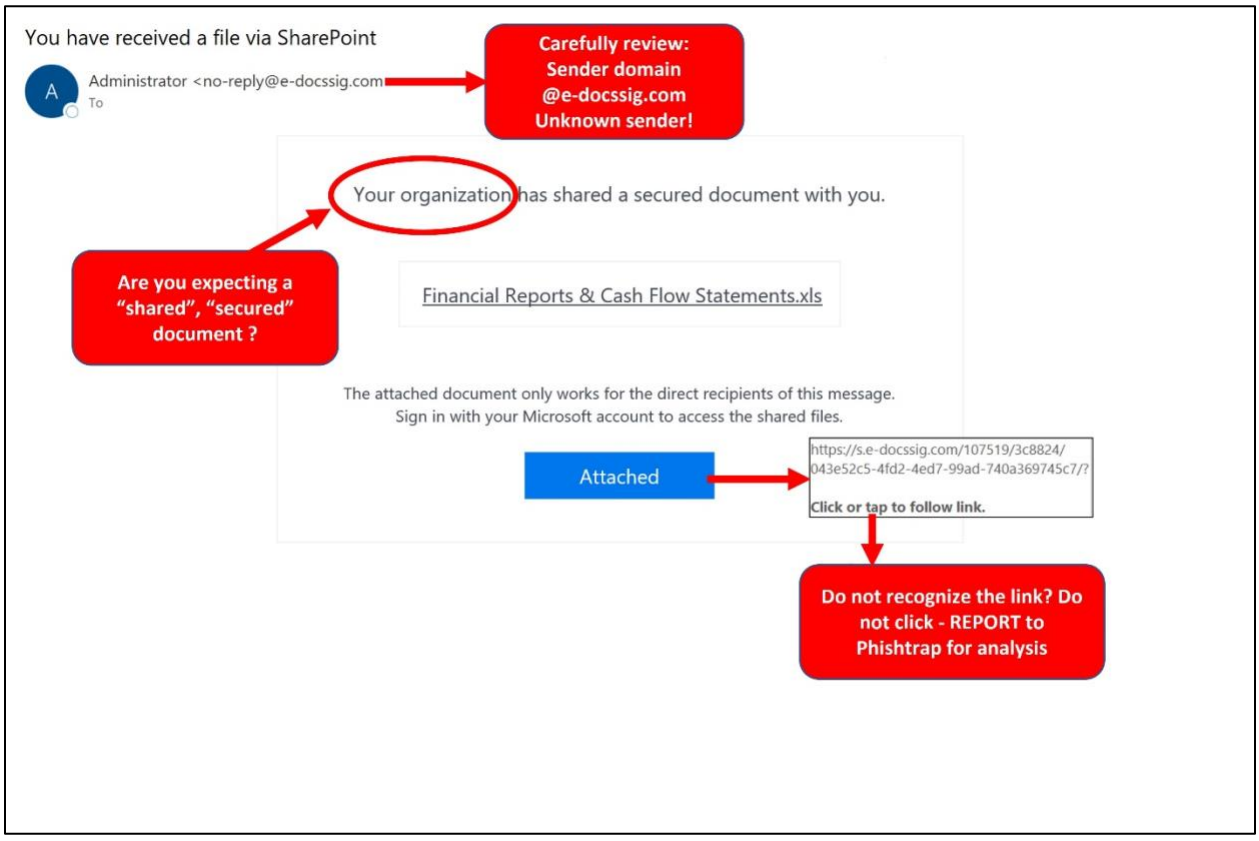
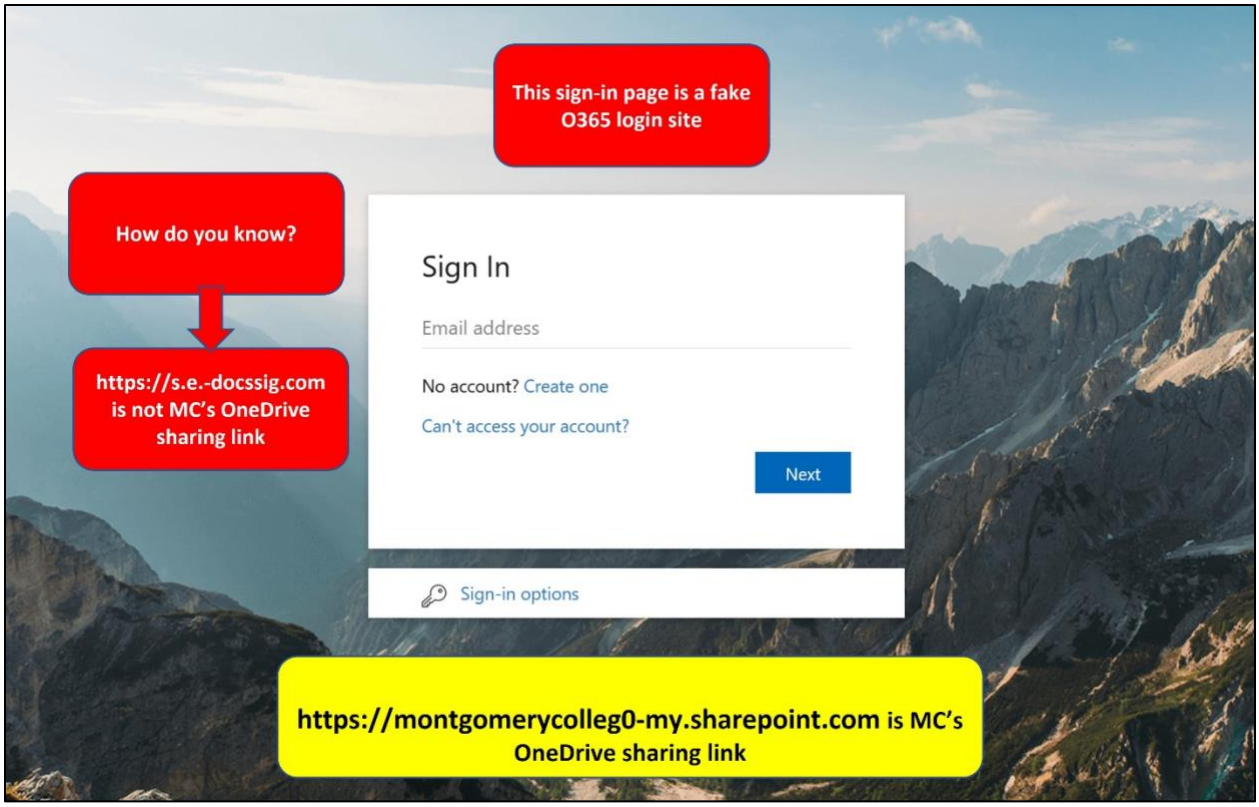
January Phishing Results: SharePoint File

The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *You have received a file via SharePoint*, which prompted you to click on a link to access the "secured" document. The attacker's intention is to capture your login credentials.

986 employees reported the phishing scenario to the Phishtrap. **Nice work MC!**

232 employees clicked the link within the training email; of these individuals, 46 entered their credentials. 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?

Let IT Security analyze the email for you - **REPORT** the email! 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 in MC Learns through Workday under the **MC Required Training** category.

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

- Do not click on "Shared" file links you are not expecting
- Expecting a shared file? Discuss with the sender what sharing platform they will be using and what sending address to expect.

- Always verify! If you know the sender, but the email seems out of context, follow up with a quick phone call.
- Check your emotions. Do not be curious and investigate the link – **REPORT** the email.
- 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.

If you have any questions or concerns regarding this process, 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