Phishing Results: Shared Dropbox Document
November 2022

The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *Dropbox Document*. Shared document phishing emails with generic or very little context provoke the recipient's curiosity. This is by design as cybercriminals expect you to click the link to discover more information. The link in this type of phishing email often leads to a fake Office 365 login page that prompts you to enter your MyMC password.

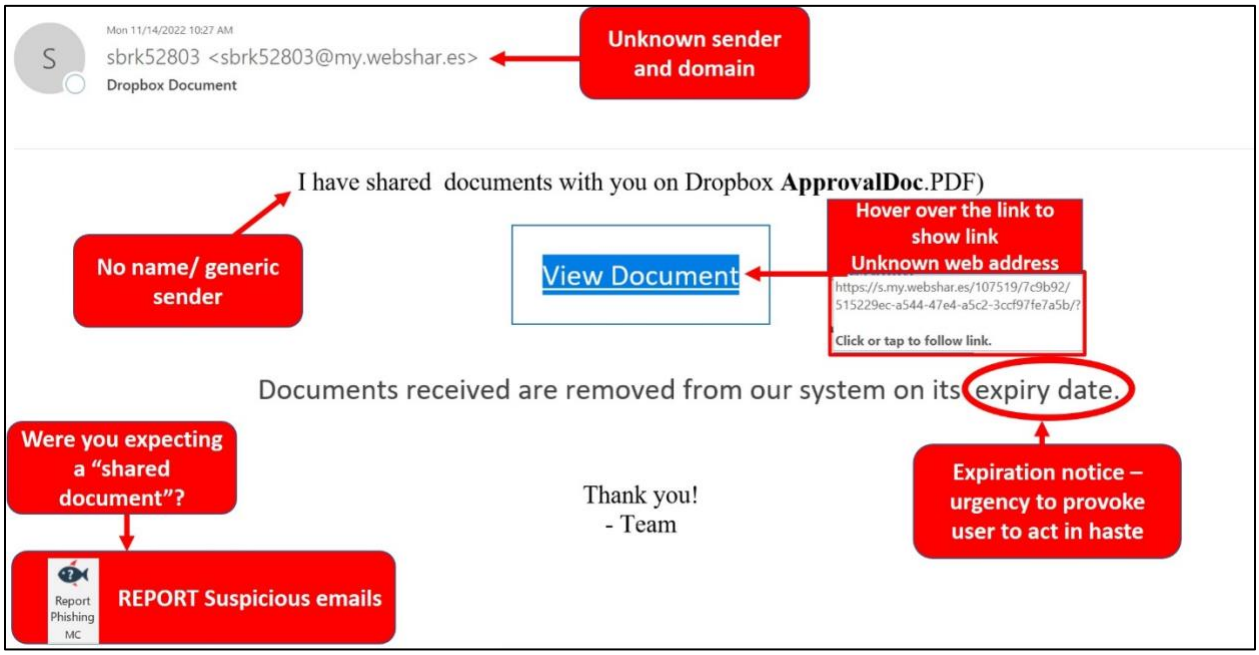
Don't be caught off guard with shared document emails. Follow these rules:

- If you are expecting a shared document:
  Ask your colleague what cloud storage service they use and for any other identifying subject matter to look for in the email.
- If you are **not** expecting a shared document:
  REPORT the email. Do not click on the link to investigate on your own.

Good news: 988 employees reported the phishing scenario to the Phishtrap. **Nice work MC!**

Opportunity for improvement: 131 employees clicked the link within the training email.
Did you click? In a real-world phishing attack clicking the link may have prompted you to give up your login credentials.

Please review the clues and tips within the email to help you identify this message as suspicious.



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.

Follow these additional tips to avoid phishing scams:

- Question any email request that is asking for your login credentials.
- Check your emotions. Do not be curious and investigate the link – **REPORT the email**.
- Keep your MC business limited to your MC email address and use your personal email address for personal business.
- Always verify! If you know the sender, but the email seems out of context, follow up with a quick phone call.

If you have any questions or concerns, 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