Phishing Results: Scan to Email Scam

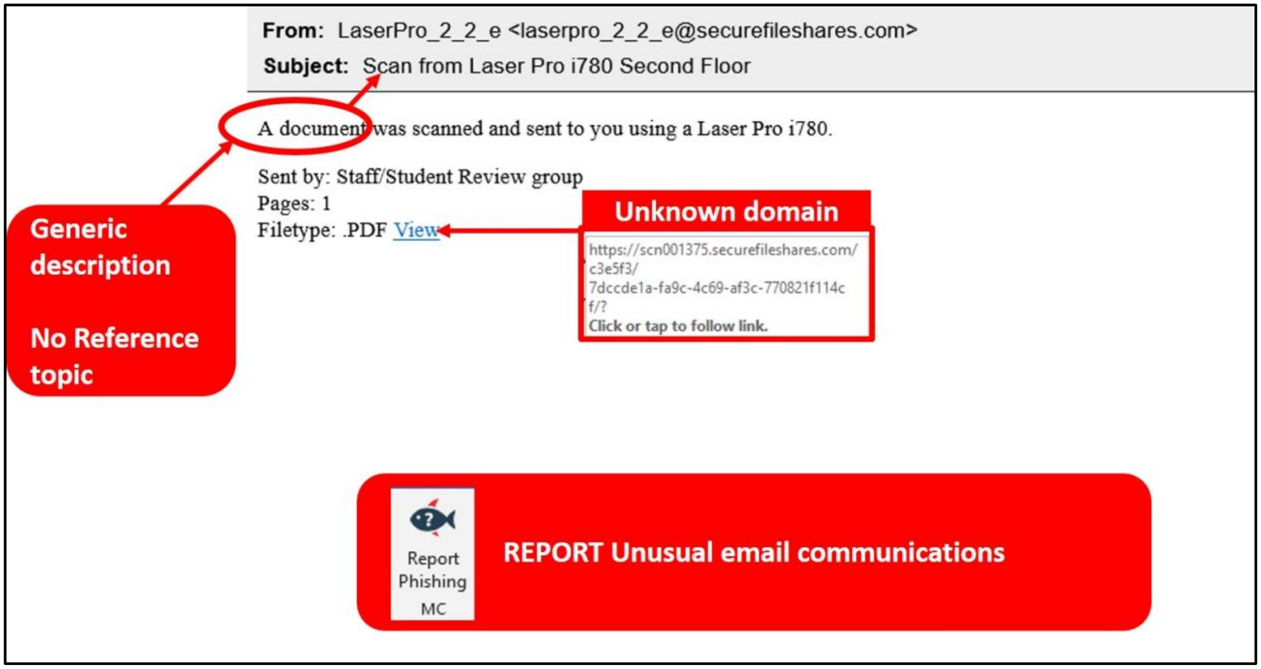
The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *Scan from Laser Pro i780 Second Floor*. This email was from an unknown, external sender and implies the email was sent by an internal printer. The email provided a link for the recipient to "View" a PDF file.

Scan to email phishing scams often provide an attachment laced with malware or a link that prompts for your login credentials. The unknown identity of the sender and lack of subject content is intentional to provoke the recipient to seek further identifiers by clicking the link or downloading the attachment. **Don't let your curiosity outweigh the security of your MC account and data!**

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

147 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.



From: LaserPro_2_2_e <laserpro_2_2_e@securefileshares.com>
Subject: Scan from Laser Pro i780 Second Floor

A document was scanned and sent to you using a Laser Pro i780.

Sent by: Staff/Student Review group
Pages: 1
Filetype: .PDF View

https://scn001375.securefileshares.com/c3e5f3/7dccde1a-fa9c-4c69-af3c-770821f114cf/?
Click or tap to follow link.

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:

- 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.
- 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