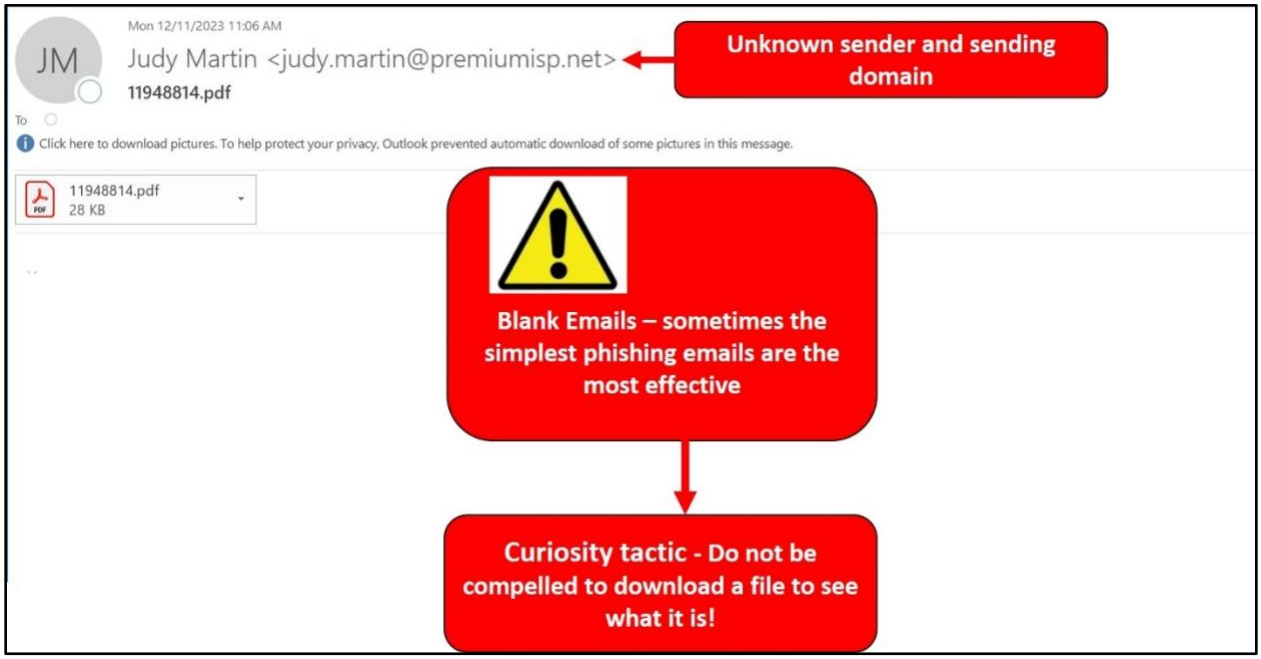
December 2023 Phishing Scenario Results

The Office of Information Technology (OIT) strives to educate the MC community on safe computing habits and security awareness topics in order to safeguard College and user data. OIT randomly sends simulated phishing email scenarios with the purpose of promoting security awareness and help users recognize phishing attempts. Our goal is to achieve **zero clicks** on real and simulated phishing emails.

The **December** phishing scenario used an emotional trigger of curiosity to test employee susceptibility by providing no content in the body and included a .pdf attachment. This simulated phish presented a useless title, "1198814.pdf", that only compounded the lack of information attackers use to invoke your investigative senses and prompt you to download the attachment.

Phishing emails that contain attachments may have a link within the attachment that lead to a malicious website, OR the attachment may contain ransomware that is executed upon download, infecting your system and the MC network. Learn more on the impacts of ransomware and the basic precautions to take.



Good News:

1,078 employees reported the phishing scenario to the Phishtrap. **Nice work MC!**

Opportunities for Improvement:

29 employees clicked the link within the training email. One click is one too many - one click puts the entire MC network at risk!

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 red flags within this type of phishing attack and to learn ways to spot a suspicious email. Visit the MC Phishing page to review the red flags within this type of phishing attack and to learn ways to spot a suspicious email.

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:

- by email at itservicedesk@montgomerycollege.edu
- by web chat on OIT's web page
- by phone at 240-567-7222