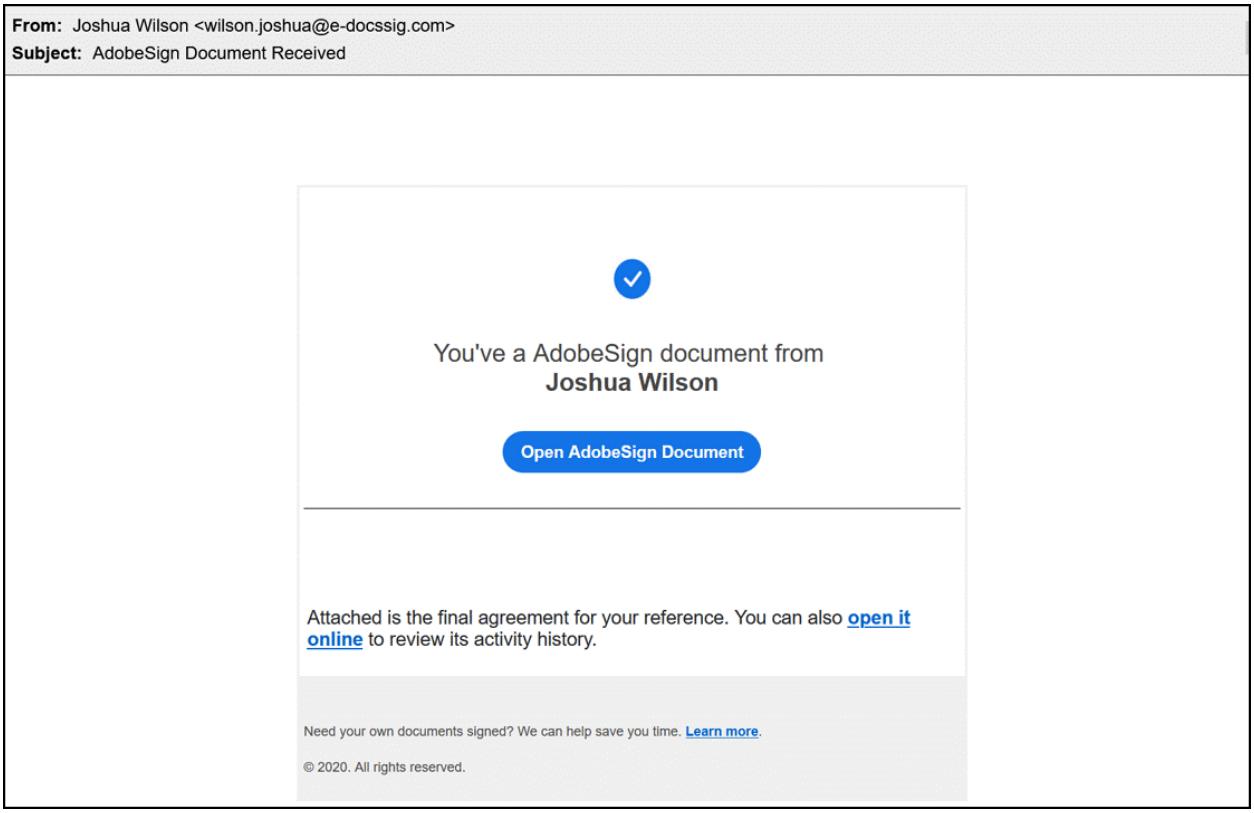
2023 MC Phishing Pro Tournament Results
October 9 – 13, 2023

IT Security kicked off October National Cybersecurity Awareness month with the inaugural Phishing Pro tournament. The tournament results are impressive – **407** employees achieved Phishing Pro status! As a recap, one phishing scenario was sent each day from October 9 to 13. The goal was to catch the simulation phish each day by NOT clicking the link and reporting the phish. Here is the complete scenario breakdown:

Day 1 – AdobeSign Document Received

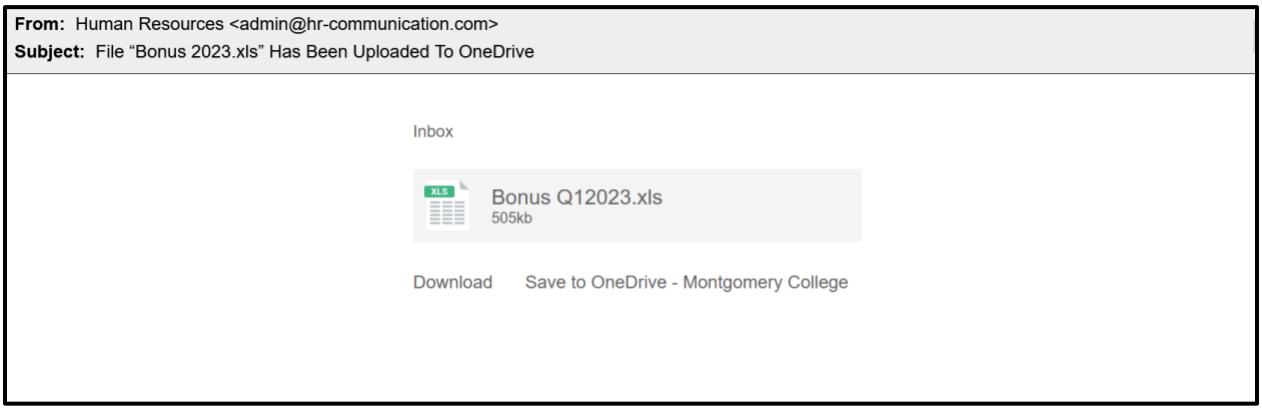
Reported: 887
Clicked: 147



The goal of this scenario was to alert employees on how legitimate digital signing services, such as Adobe DocuSign, are used to trick you into clicking the link. Upon opening the link, a fake login page is presented requesting your login user name and password. Don't be fooled by this Adobe look-a like. Expecting an electronically signed document request? Check with the sender on the logistics and details of what to expect. Not sure of the email? Report it using the Report Phishing button.

Day 2 - File "Bonus 2023.xls" Has Been Uploaded To OneDrive

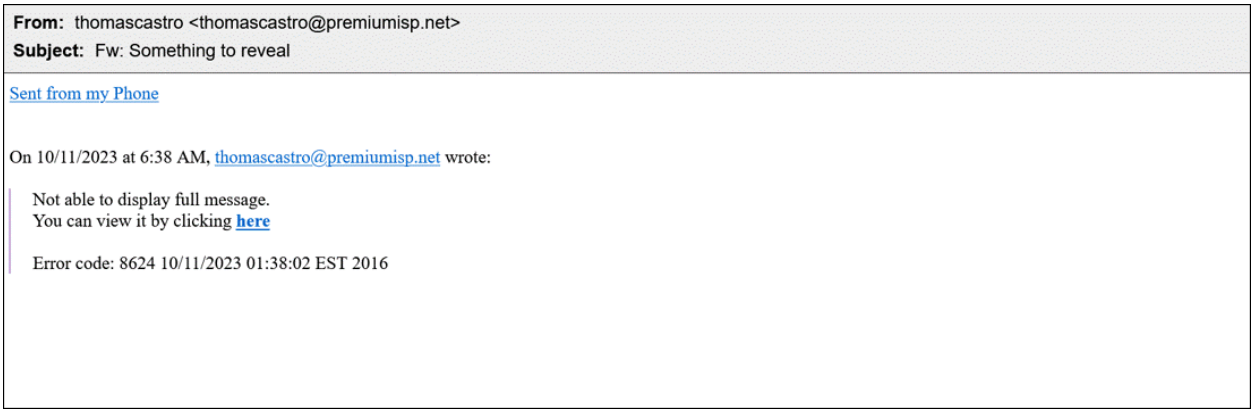
Reported: 942
Clicked: 200



Did the email subject "Bonus 2023…" pique your interest? Scammers know the right words to include in order to convince you to open or download an attachment. Moreover, they know that by adding "Montgomery College" to the body of the message will boost the legitimacy of the email. This type is a malware attack. Malware is software with malicious intent used to gain unauthorized access or lock up the device by encrypting the data as in the case of ransomware. Stay alert to receiving unusual emails especially those that are vague and have attachments.

Day 3 – Something to reveal

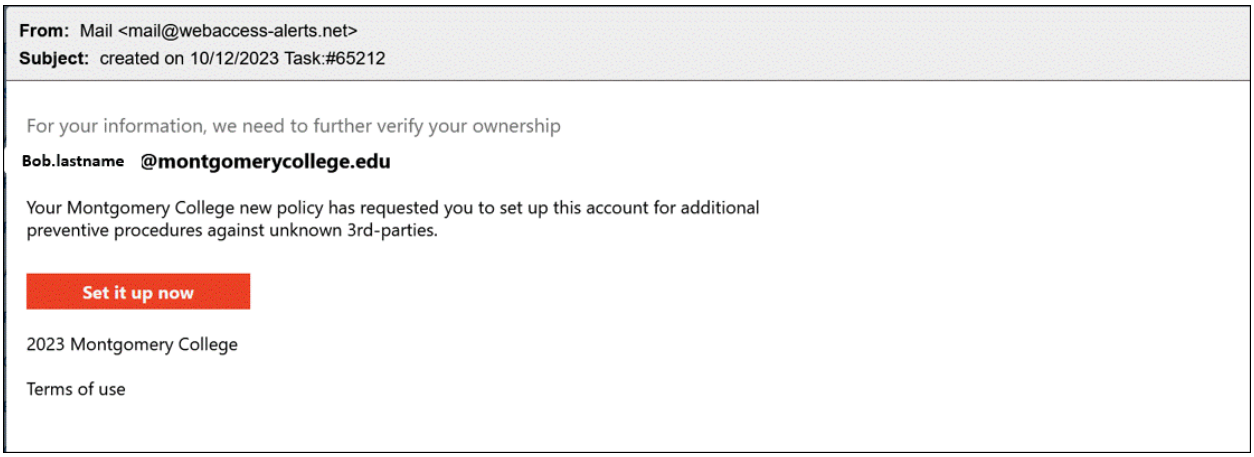
Reported: 1095
Clicked: 12



MC employees spotted this phish with ease! Messages with limited information or direction provoke action upon the recipient to search for details in the attachment or to follow the link. This phishing email is vague, from an unknown sender, and not expected. Save yourself the time in analyzing and report suspicious and unusual emails.

Day 4 – created on 10/12/2023 Task:#65212

Reported: 1255
Clicked: 41 clicked ; 11 out of those 41 submitted their login credentials



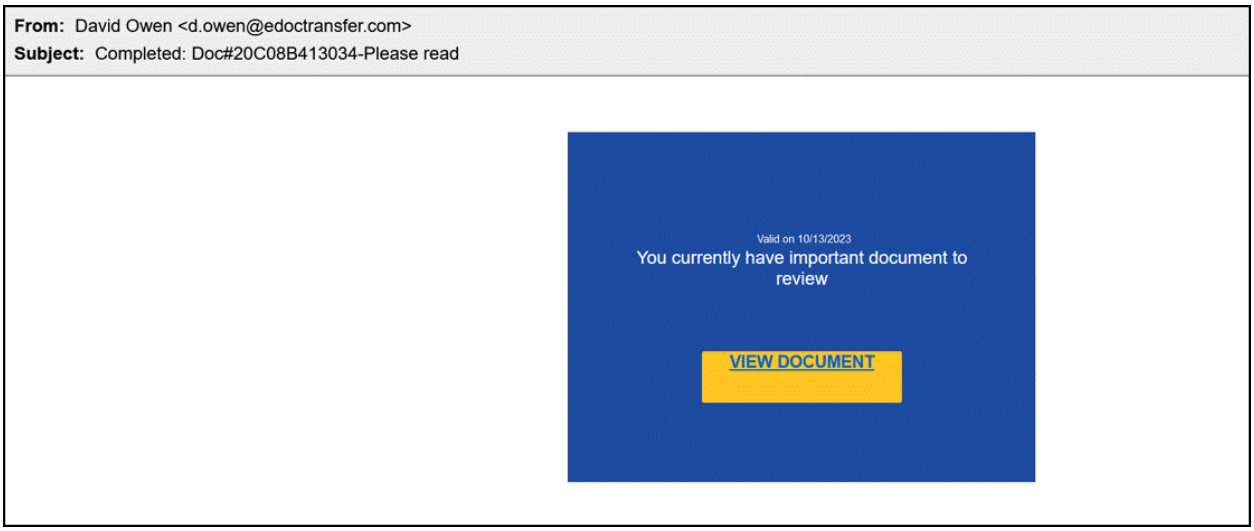
The most common phishing email is one crafted to steal your login credentials. To avoid this type of attack, remember these three tips:

- Inspect the website address – hover your mouse over the link to reveal the web address.
- Use bookmarks to navigate to trusted sites.
- Guard your credentials. Keep your usernames and passwords private. Pause and be sure of the login website before entering your data.

Credential harvesting phish are one of the most damaging types of phish. Once you give up your password the attacker is free to login to your account. MC's solution to protecting user accounts is twofold – educate employees on the threat and prevent unauthorized access with Two-Factor Authentication (2FA). Remember, only authorize 2FA login attempts/prompts you initiate. Deny unauthorized attempts using the Duo Mobile app.

Day 5 – Completed: Doc#20C08B413034-Please read

Reported: 896
Clicked: 71 clicked; 18 of those 71 submitted their login credentials



This was the last phishing email in the five-day tournament - another electronic document with credential harvesting. The same rules apply – if you were not expecting the email, do not click the link and do not investigate on your own.

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.

We encourage employees needing assistance identifying threats to take the **required Data Security@MC training** found in Workday MC Learns.

As always, 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