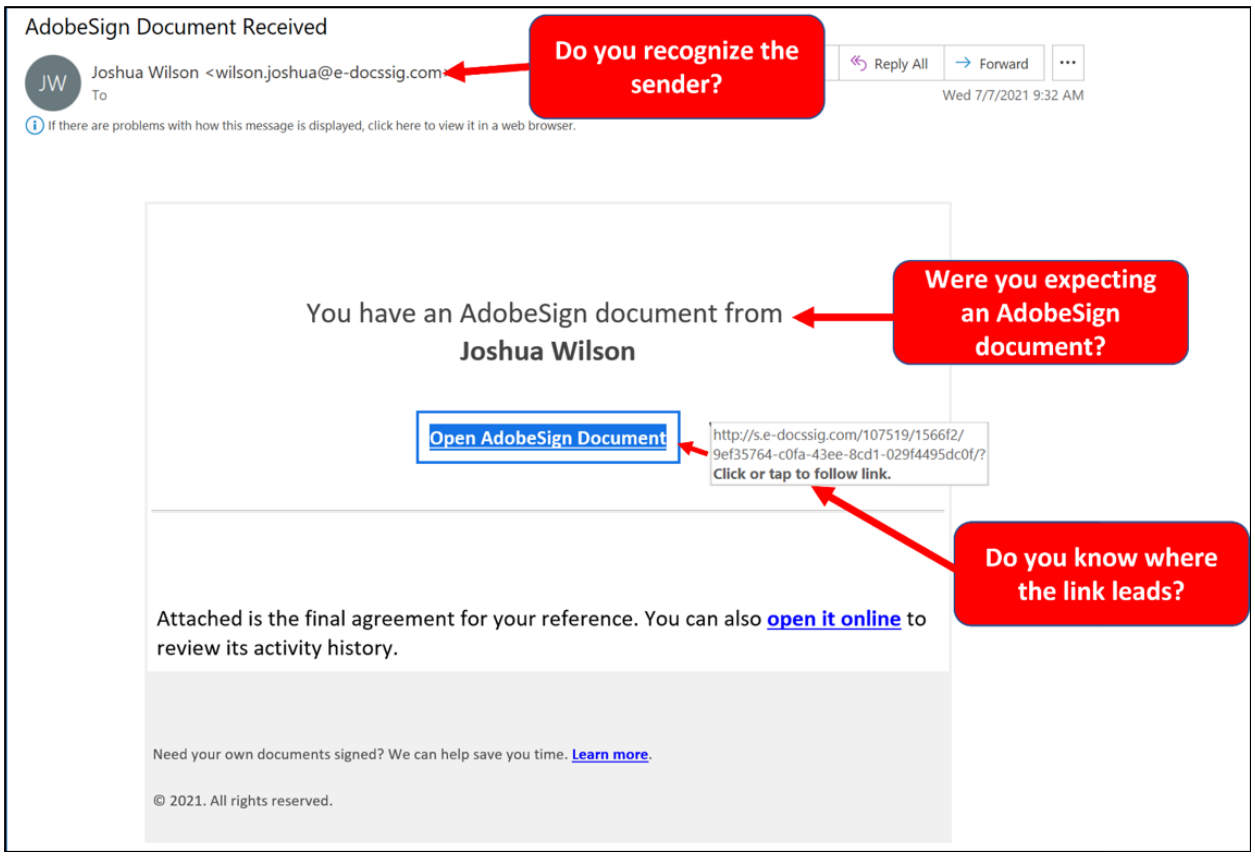
The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *AdobeSign Document Received*, with a link to "open" the document. This type of phishing scam is used to capture employee login credentials. The generic email set up is intended to provoke curiosity. The attacker's lure is to reference a "final agreement" indicating a previous [fake] communication. There are legitimate secure signing applications and services available to consumers. If you are expecting a document that requires a secure signature, check in advance with the sender on what product/service they will be using.

926 employees reported the phishing scenario to the Phishtrap! Reporting is the preferred action as it provides IT Security the threat intel it needs to respond.

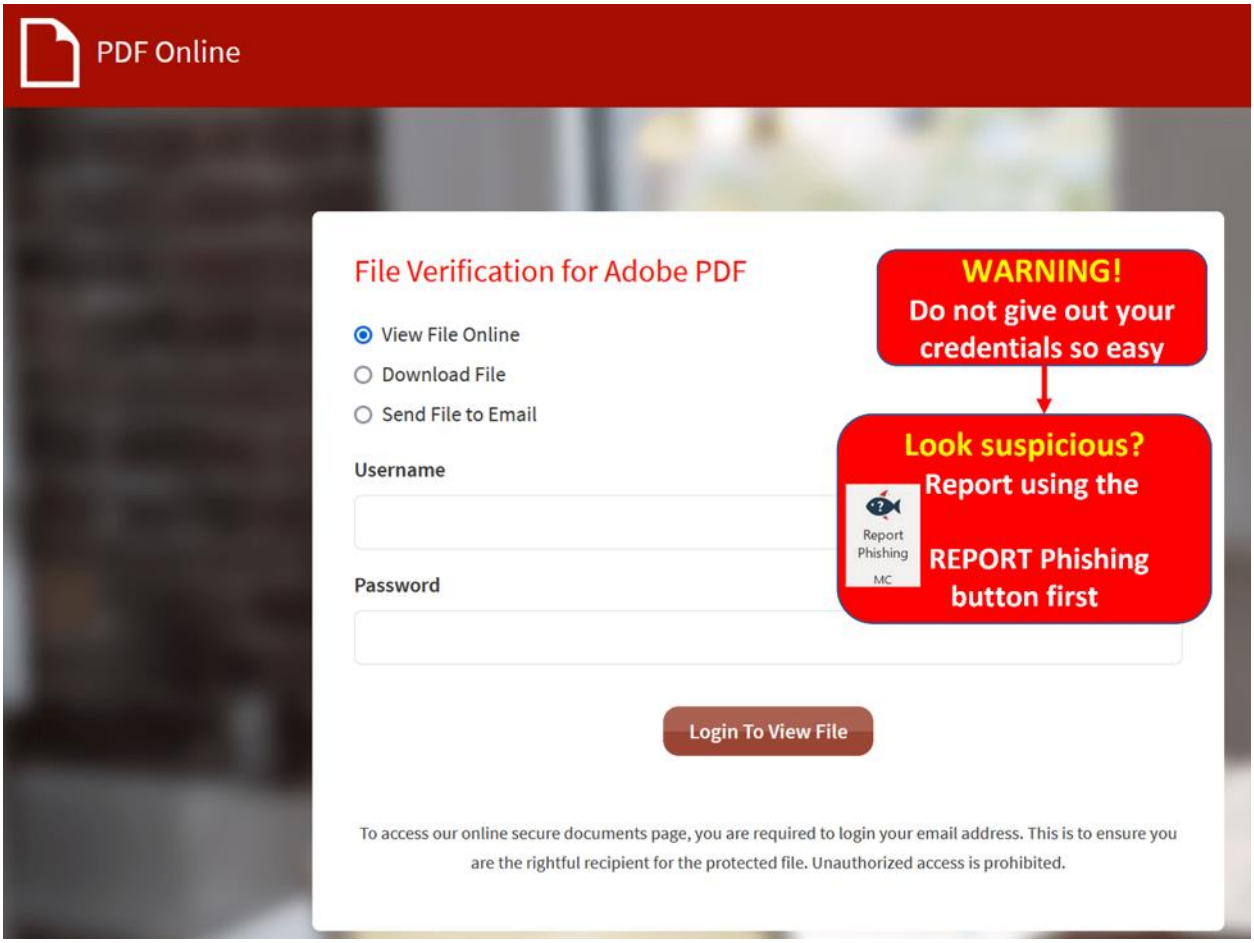
293 employees clicked the link within the training email; of these individuals, 32 entered their credentials. There were several clues within the email to help you identify this message as suspicious.

Please review the email again and pay close attention to the red flags:



- If you do not know the sender, i.e., *Joshua Wilson*, do not click on the link.

- Expecting a document? **293 employees clicked the link!** In a real phishing email the link would lead to a credential harvesting site:



The links are often difficult to discern where they lead – if you are expecting a document check with the sender and ask what service they are using.

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 Outlook allows you to quickly report suspicious emails to IT Security.

If using Office 365 on the web, follow these steps to pin the Reporter Button to your email message surface. 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:

- 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.
- Be cautious. Malicious actors and aggressive spammers are attempting to take advantage of our new normal by **preying on our stress levels and hoping our guard is down with COVID-19**, gift card, meeting invites, shipping notices, and stimulus check scams.
- 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