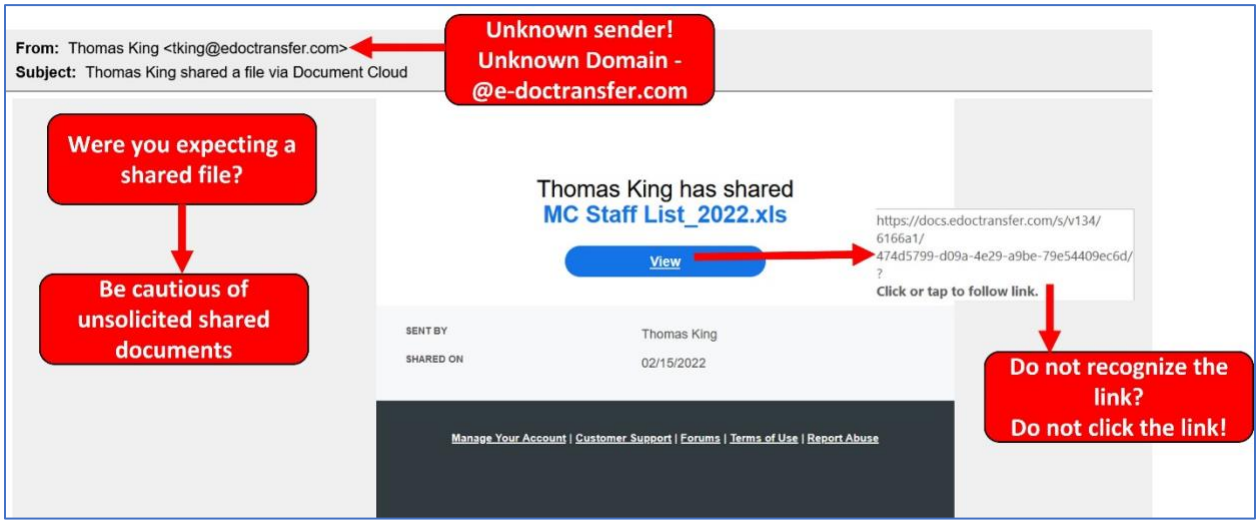
February Phishing Results: Beware of Office File Macros

The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *Thomas King has shared MC Staff List_2022.xls*. The email included a clickable link to "view" the file. Microsoft Office allows users to create macros to automate repetitive tasks in files created with applications such as Excel or Word. Macros include commands or scripts that run on your computer. Unfortunately, macros are often exploited by attackers and are the most common method phishers use to deliver malware.

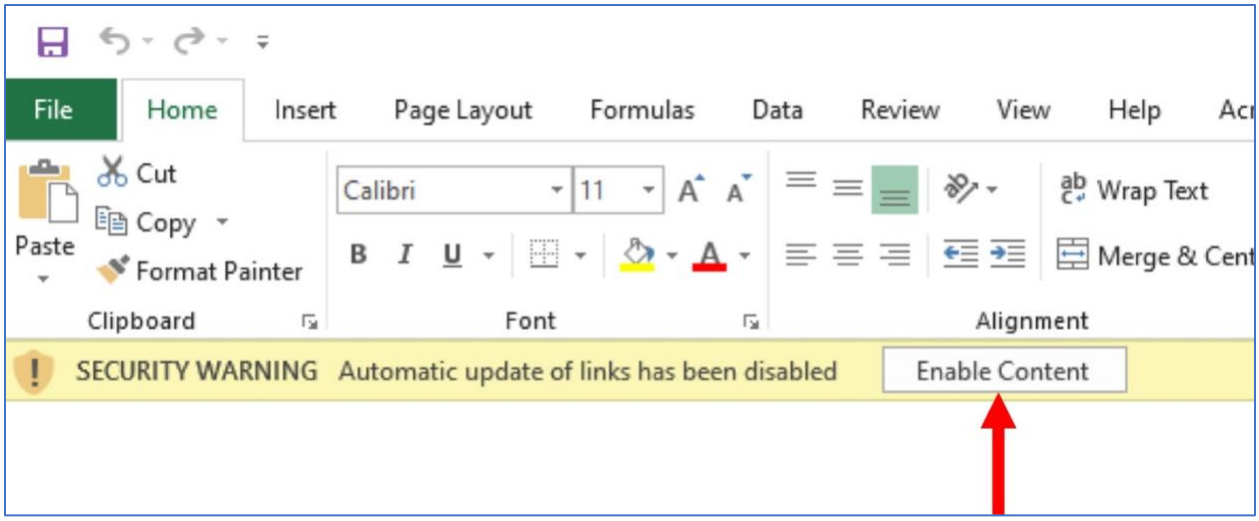
864 employees reported the phishing scenario to the Phishtrap. **Nice work MC!**

175 employees clicked the link within the training email. Did you click? *In a real-world phishing attack you would have introduced malware to the College's computing environment.*

There were several clues within the email to help you identify this message as suspicious. Please review the red flags below:



Keep macros disabled! Dangers in macros:



- **Open the door to your computer**
  All it takes is one click to enable macros. Once enabled, the macro has full permission to execute malicious commands on your computer.
- **Distribute dangerous forms of malware**
  Once you enable macros, most malicious attachments will download other types of malware from a remote server, like ransomware or spying software.
- **Evade email filtering protection**
  Dangerous files that contain macros can bypass spam filters and anti-virus scanners. This is because the malware isn't actually there until the macros are run and the malware is downloaded.

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.

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.

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.

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.