October 2020 Phishing Exercise Recap: We Have Work To Do

National Cybersecurity Awareness Month (NCSAM) is ending soon, but cybersecurity awareness and education should be practiced all year long. Visit IT Security's Cybersecurity Awareness webpage for tips and resources to **Do Your Part. #BeCyberSmart**.

During this period of remote work, employees are even more susceptible to cyber threats, and the latest phishing scenario results show that vulnerability.

 **Good News: 717 employees reported the phishing scenario email**, *Incoming Emails Rejected.*

Thank you for being vigilant and protecting yourself and the College! Your skepticism in responding to email allows IT Security to quickly identify malicious email and take appropriate action to prevent any damage.

 **Bad News: 682 employees clicked the link!**

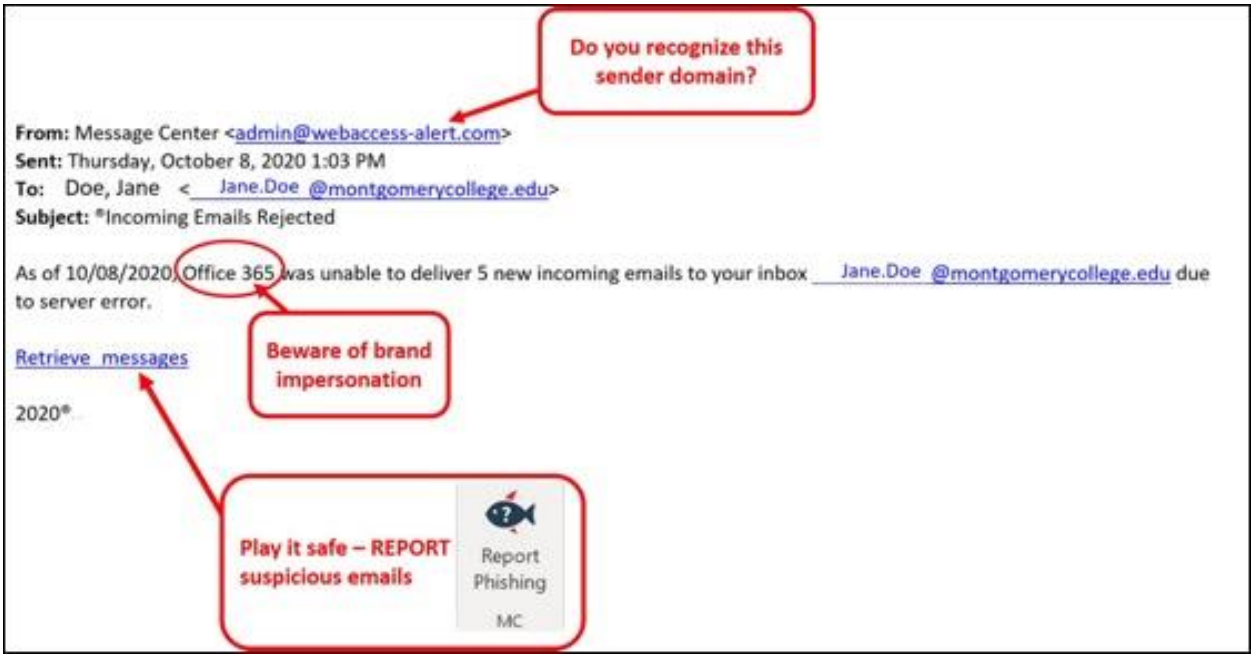
In a real phishing email these employees would not only be giving up their account privacy, but potentially causing real harm to the College:

- Allow the attacker to send additional phishing emails as if they came from you
- Allow the attacker to steal sensitive College data
- Introduce ransomware, encrypting your workstation and other key systems, making them unusable
- Cause disruption in College business

Be skeptical: Think Before Your Click!

The Office 365 impersonation themed scenario prompted users to click a link to "Retrieve messages".

Please review the clues within the email to help you identify a phishing email.



What should you do if you suspect an email may be a phishing attempt?

REPORT the email! Educated employees are our last line of defense to thwart phishing attacks and help us prevent data breaches. 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 through MC Learns.

Below are some common clues to look for in identifying a suspicious email:

- Be wary of some of these additional credential theft subjects used in Phishing attempts: Account Security Alert, Expired Password, Inbox over the limit, Undelivered messages.
- Check your emotions. Beware of emotional triggers such as an urgent deadline for completion or severe consequences if the request is not complete -i.e. follow MC processes and procedures.

- 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, 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.
- Remember - phishing emails are the preferred method among attackers because it is the easiest way to get your login credentials. Don't give them the opportunity.
- The message is overly generic, the request is outside of your scope of responsibility, and/or the action requested is not typical of a current business process.

For any technology-related questions or issues, 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